Sustainable Futures 12 (2026) 102036

Contents lists available at ScienceDirect

Sustainable Futures

journal homepage: www.sciencedirect.com/journal/sustainable-futures

Mapping current and potential criminal and security issues associated with climate change mitigation technologies

Sarah Y. Zheng [a,b,*], Shane D. Johnson [a,b], Paul Ekblom [a], Mark A. Maslin [c], Hervé Borrion [a], Lauren Young [d,f], Manja Nikolovska [a,b,e], Matthew P.J. Ashby [a], Lorenzo Pasculli [a,b]

[a] Department of Security & Crime Science, UCL, 35 Tavistock Square, London, WC1H 9EZ, United Kingdom
[b] Dawes Centre for Future Crime, UCL, 35 Tavistock Square, London, WC1H 9EZ, United Kingdom
[c] Department of Geography, UCL, North West Wing, Gower Street, London, WC1E 6BT, United Kingdom
[d] Global Initiative against Transnational Organized Crime, Avenue de France 23, Geneva, CH-1202, Switzerland
[e] NYU Shanghai, 567 West Yangsi Rd, Pu Dong Xin Qu, China
[f] Durrell Institute of Conservation and Ecology, University of Kent, Canterbury, CT2 7NZ, United Kingdom

ARTICLE INFO

Keywords:
Climate change mitigation
Crime prevention
Security risk

ABSTRACT

Our transition to a low-carbon future critically depends on technologies to mitigate climate change (CCMTs). These include renewable energies, carbon capture, utilisation and sequestration (CCUS), and electric vehicles. As many of them are still evolving technologies, they will likely present novel crime and security risks. Unfortunately, knowledge about such risks is still limited and fragmentary. This scoping review aims to bridge this gap and inform policymakers to prevent such emerging risks. We found 97 relevant articles from a total of 1139 papers we screened from academic and non-academic sources across disciplines. They revealed 20 distinct crime threats of six different natures: property offences, cyber-attacks, financial crime and corruption, environmental threats, human rights abuse, and national security threats. Notable examples of criminogenic situations are CCUS-related environmental threats, greenwashing, and territorial conflicts over "green projects" that require adequate future crime prevention strategies. To that end, we also found 22 (potential) countermeasures, mostly of a legal or policy nature. This comprehensive overview highlights what appears to be an under-researched aspect of sustainable development, which we believe should include ensuring safety and security throughout climate mitigation supply chains.

1. Introduction

Technology plays a fundamental role in addressing climate change. In particular, a broad set of technologies known as "climate change mitigation technologies" (CCMTs) can help reduce the long-term increase in the Earth's surface temperature attributable to global warming to a maximum of 1.5°C, as required by the UN Framework Convention on Climate Change (UNFCCC; also known as "the Paris agreement") (Fawzy et al. [1]). CCMTs seek to slow and decrease greenhouse gas (GHG) emissions, either by reducing GHG sources or by capturing and storing GHGs or absorbing them in natural sinks (UN Framework Convention on Climate Change (UNFCCC) [2]; European Environmental Agency [3]; Fawzy et al. [1]). Examples include technology suites for carbon capture, utilisation and sequestration (CCUS), smart energy grids that facilitate renewable energy supplies, hydrogen-powered transport and electric vehicles (Napp et al. [4]).

Mitigation technologies are rapidly evolving and are expected to develop and spread across various countries due to a combination of market forces, political incentives, and changes to financing and international law. For example, the UNFCCC sets clear legal obligations for state parties to promote and cooperate in the development, application, diffusion, and transfer of environmentally sound technologies to control, reduce or prevent carbon emissions (Article 4 UNFCCC (UN Framework Convention on Climate Change (UNFCCC) [2]). Dedicated UN mechanisms, such as the UNFCCC Technology Mechanism and the UNFCCC Financial Mechanism, are supporting the development and transfer of climate technologies, especially in developing countries. Like other climate initiatives, such technologies can play a crucial role in promoting sustainable development (Coenen [5]). The linkages between climate and development are explicitly enshrined in both the Paris

* Corresponding author at: Department of Security & Crime Science, UCL, 35 Tavistock Square, London, WC1H 9EZ, United Kingdom.
E-mail address: sarah.zheng.16@ucl.ac.uk (S.Y. Zheng).

https://doi.org/10.1016/j.sftr.2026.102036
Received 20 November 2025; Received in revised form 8 May 2026; Accepted 16 July 2026
Available online 25 July 2026

agreement and the 2030 Agenda for Sustainable Development or Sustainable Development Goals (SDGs) (Gomez-Echeverri [6]). So much so that, climate action as well as access to affordable and sustainable clean energies are amongst such goals (SDG 7 and 13, respectively). However, while researchers continue to study the effects of climate technologies on the environment and private companies explore business and investment potential, the crime and security implications of CCMTs have so far been under-explored. For example, the 2023 Intergovernmental panel on Climate Change (IPCC) synthesis report does not mention crime at all, while references to "security" in the report only concern natural hazards (e.g., food, energy or water security)—not malicious or clearly criminal threats [7]. This omission is especially surprising given that security (also from crime threats) has been long recognised as a necessary condition for sustainability (WCED [8]; Clifton [9]; Salas Alfaro et al. [10]). Peace, justice and strong institutions are also sustainable development goals (SDG16), together with other principles of human security such as wellbeing, equality, education and work (e.g., SDGs 1–5, 8, and 10).

The expected criminogenic effects of such technologies are many and multifaceted. At a basic level, climate technologies themselves can be targets or instruments of criminals that seek to misuse, misappropriate or damage them. Some core examples are the various cases of solar panel theft widely reported in the media (Dutton [11]; Connell [12]; Norman [13]) or terrorist attacks on water resource management systems (cf. Gleick [14]). Yet, there can be more complex criminogenic effects. Climate technologies are reshaping the immediate environments in which they operate (e.g., farming processes and practices, carbon sinks), as well as the broader societal, financial and business environments that provide the resources to develop, manufacture, disseminate and commercialise technologies. For instance, the introduction of national or international subsidies, grants or tax reliefs and concessions to encourage the production or use of CCMTs can attract corruption, fraud, and other financial crime. The Northern Ireland Renewable Heat Incentive (RHI) scandal is an example of this (BBC News [15]). The availability of financial or natural resources can also fuel conflict and human rights violations, as has been evident for decades in the mining industry.

Thus, understanding the potential crime and security risks associated with CCMTs is imperative to facilitate our transition to a sustainable future. Since a comprehensive overview is lacking, this study presents a scoping review of academic and grey literature from any discipline that brings together previously described crime threat scenarios and (potential) countermeasures. Out of over 1100 screened articles, 97 were included, and any identified crime and security risks, as well as potential countermeasures were grouped by theme and analysed qualitatively. These findings will help researchers and policymakers shape future-proofing regulations, and inform future research and technological development priorities to ensure that technologies developed to combat climate change do not become unintended "crime polluters" (Eck and Eck [16]).

1.1. Climate change mitigation technologies: functional categories

Climate change technologies have different objectives. Some focus on mitigation, others on adaptation. Whereas climate change mitigation technologies (CCMTs) seek to reduce greenhouse gas (GHG) emissions, adaptation technologies aim to make appropriate adjustments and respond to the impacts of climate change by reducing negative effects or by exploiting the positive ones (UN Framework Convention on Climate Change (UNFCCC) [2]). These include a broad range of technologies, many of which are already in common use, such as dykes to protect land from flooding, early warning systems for weather change, and air conditioning (UN Framework Convention on Climate Change (UNFCCC) [2]). Mitigation technologies, by contrast, range from fairly commonly used solar panels and lithium-ion batteries, to less widespread electric arc furnaces and CCUS methods that are frequently still in research and development stages. Note that (solar) geoengineering technologies that aim to reduce the global temperature by reflecting back sunlight or other interventions to regulate global thermodynamics do not address GHGs, and therefore are considered out of scope.

Given the variety of technologies that aim to mitigate climate change, it is helpful to consider them in terms of their functionality. Fawzy et al. [1] distinguish two functional categories: 1. CCMTs that provide alternatives to fossil fuels, thus preventing future carbon emissions; and 2. "negative emission" technologies, which are comprised of CCUS techniques that seek to reduce existing greenhouse gases in the atmosphere. The first category can be split into energy generation (e.g., wind, solar, geothermal) and energy use (e.g., electric cars, hydrogen steel production). Negative emissions technologies can be split into CCUS at source (e.g., carbon capture in industrial manufacturing processes) and atmospheric (e.g., direct air capture), where atmospheric CCUS can be split further into biological and non-biological. Although many of both types of mitigation technologies are still in development, they have the potential to help us become independent from fossil fuels and reduce the net volume of GHGs in the atmosphere.

1.2. Potential for crime harvests from CCMTs

Despite their intended purposes, CCMTs are likely to unintentionally create new opportunities for crime. The introduction of any new technology can facilitate the convergence of criminogenic conditions (i.e., motivated and well-equipped offenders, suitable targets and the absence of anyone who can stop a crime occurring) by altering our routine activities (Johnson [17]; Cohen and Felson [18]), by providing new crime targets for motivated offenders, which may include new avenues to access those targets. Unfortunately, in the anticipation of new technologies, crime and security implications are often overlooked and, hence, the implementation of appropriate countermeasures becomes reactive (Pease [19])—especially when foresight into likely future crime risks is absent. Since offenders often seek to maximise rewards while minimising efforts and risks of detection (Cornish and Clarke [20]), the availability of new targets and the (temporary) absence of effective controls can precipitate offenders' motivation to "harvest" any new crime opportunity (Pease [19]). "Crime harvests" have been observed for various new technologies, such as automobiles in the nineties (Laycock [21]) and, more recently, the metaverse (Gomez-Quintero et al. [22]), social robots (Zheng et al. [23]) and cryptocurrencies (Akartuna et al. [24]).

Such crime harvests can be expected for CCMTs too. While not all CCMTs are new (e.g., solar panels first began to be adopted in the 1950s), the current socio-political and legal context commands wide and rapid adoption. Driven by urgent climate targets, public demand, and supportive legislation, many governments and industries are now required to accelerate the deployment of these technologies. However, this pressure risks neglect of important crime and security aspects.

A case in point, the criminal exploitation of carbon trading markets in the early 2000s highlights the convergence of motivated offenders, suitable targets, and the absence of capable guardianship. In this case, motivated fraudsters were quick to identify carbon credit markets as suitable targets for fraud, as carbon offsets were easily transferable financial products that were poorly monitored (Williams [25]; McKie et al. [26]). The lack of robust oversight, the presence of regulatory loopholes, and inconsistent enforcement across jurisdictions created a vacuum of capable guardianship, enabling fraudulent activities such as VAT fraud, double-counting, and the sale of non-existent credits. This convergence created ideal conditions for criminal exploitation within a system intended to incentivise carbon reduction.

Similar examples include opportunities for the theft of high-value components of solar panels (e.g., precious metals), electric vehicles (and their lithium batteries), and wind turbines that may be deployed in remote or unsecured locations (i.e., lack of guardianship), making them vulnerable to theft, vandalism and sabotage [13,27,28]. The supply chains of these components (which include the rapid scaling up of critical mineral sourcing) often intersect with (developing) regions plagued by illegal mining, labour exploitation, conflict and violent crimes involved in controlling said supply chains ([29]; Bernards [30]). In line with the crime harvest concept, the surge in demand for these resources (and the resulting increased profitability), critical to the development of CCMTs, will exacerbate the context for motivated criminals. These examples show that while climate change mitigation technologies aim to solve environmental problems, they also alter the social and economic landscape in ways that generate new criminal opportunities. Anticipating these "harvests" can help policymakers and law enforcement design and implement proactive regulatory and protective measures before a crime harvest occurs, rather than reacting after one has already taken place. Anticipating a crime harvest is also important, because designing security into a new product or system from the outset ("security-by-design" practices) is often both less expensive and more effective than attempting to retrofit security measures later on (Tuptuk and Hailes [31]).

1.3. Towards a sustainable future, safely

The relationship between climate mitigation and sustainable development (defined here as "development that meets the needs of the present without compromising the ability of future generations to meet their own needs'' (WCED [8]) is a complex one. A 2022 report by the IPCC emphasises that accelerated climate mitigation is critical to sustainable development as it can contribute to achieving many SDGs, but it can also entail some trade-offs. These include, for instance, adverse effects of mitigation technologies on biodiversity, natural resources or local populations in terms of employment or access to energy, food and water (IPCC [32]). The idea of "trade-offs" implies a potential conflict between the principles of climate mitigation and those of sustainability, that policymakers can hope to resolve by accurately balancing competing values and interests, as suggested by the IPCC's report. As such, trade-offs are expected and somewhat acceptable. On the other hand, any crime and security threats enabled by climate change mitigation technologies cannot be considered mere trade-offs between competing values or interests, but rather to unintended consequences that violate all such values and interests by compromising both climate action and sustainable development and are therefore unacceptable from any perspective. Moreover, the mitigation of crime and security threats requires countermeasures that go beyond a balanced design of climate policies and encompass a broader range of security interventions ranging from technological and situational solutions to regulation, law enforcement and criminal justice. In other words, the emergence of such threats further complicates the relationship between climate mitigation and sustainable development by adding a security component to it.

The association between security and sustainability or sustainable development (which are not necessarily synonymous) has long been discussed by the United Nations and the literature and it has recently gained new momentum (Malmio [33]). The extension of the notion of security beyond mere national security (i.e., the protection of the state from external military threats) enabled the realisation of the interdependence of security and sustainability: sustainability can contribute to security problems as much as security can contribute to sustainable development (WCED [8]; Salas Alfaro et al. [10]).

Despite growing attention to these issues, knowledge on the interconnections between security and sustainability or sustainable development remains still fragmented (Salas Alfaro et al. [10]) and still relegated to a conceptual or theoretical level (cf. Malmio [33]. There appears to be a lack of systematic and comprehensive investigations on the crime and security threats related to climate change mitigation technologies. Despite the vital role of CCMTs in our transition to a sustainable future, a study published in 2020 found that only 0.12% of all climate-related research funding was spent on social science (e.g., criminology) in climate change mitigation studies (Overland and Sovacool [34]). Most existing research on CCMTs focuses on technological aspects, while politicians, industry leaders and law-and policymakers who are tasked with addressing crime and security issues lack the knowledge needed to properly manage certain criminal risks, such as cyber-attacks. Although various publications mention issues around water, food and energy security, these do not address intentional (crime) threats. Furthermore, the diverse nature of CCMTs and the fragmented nature of research dedicated to the distinct technologies hinders the prioritisation of crime and security risks on climate policy and research agendas.

Given the rapidity at which climate change mitigation technologies are being adopted around the world and given the crime and security risks that this might enable, this knowledge gap is a critical shortcoming and one that needs urgent attention. This study is intended to be a step toward narrowing this gap. To do this, we systematically searched for academic and grey literature regarding the crime and security risks related to CCMTs, and any countermeasures intended to address them. The result is a comprehensive scoping literature review that identified 20 distinct crime threats and 22 potential countermeasures. These findings can lay the groundwork for future empirical and theoretical research on the relationships between climate action, sustainability and security. In the short term, they can be used directly by policymakers to future-proof legislation (Pasculli [35]) around the further deployment of CCMTs also in the context of sustainable development and with a view to achieve as many SDGs as possible, as safely as possible. Ultimately, the results of this study can contribute to shaping both a more sustainable and a more secure future.

2. Methods

To identify previously described crime and security risks related to CCMTs, we performed a scoping literature review. Like systematic literature reviews, scoping reviews rely on a pre-defined search protocol with clear inclusion and exclusion criteria.

2.1. Research objective

The main objective of this scoping review is to collect qualitative data on specific looming crime and security risks related to CCMTs. Some of these risks may have already materialised to some extent, whereas others may be speculative. Accordingly, the presented analysis will be of a primarily qualitative nature. We followed the identification, screening and inclusion stages according to the PRISMA framework (Page et al. [36]) to conduct this scoping review. First, we defined our research question using the PICo framework (Lockwood et al. [37]) to set the scope of the review:

1. *Problem:* future crime threats enabled/facilitated by climate change mitigation technologies
2. *Phenomenon of Interest:* identification, description and analysis of crime threat scenarios and possible countermeasures
3. *Context:* any sector of application, globally, in the foreseeable future (roughly upcoming 5–10 years)

By "future crime threats", we mean both new forms of crime and the manifestation of existing offences and emerging behaviours that, while not yet fitting the legal definition of existing offences, can cause harms and social concerns equivalent to those of known offences (Hillyard and Tombs [38]), and might therefore become criminalised in the future. This is particularly important for environmental or ecological threats, which we expect CCMTs to enable. These threats include practices and behaviours that might be perfectly legal, despite the harms they cause to the environment and societies, such as environmental impacts from large-scale "green projects" (McKie [39]; Lynch and Stretesky [40]; Stretesky et al. [41]). A notion of "future crime threats" that includes also harmful but not necessarily criminal or illegal activities is essential for lawmakers and prosecutors in any jurisdiction to assess whether legal definitions of existing offences need to be revised or reinterpreted, or new offences need to be introduced. Moreover, since not all offences require intent, the review covers both intentional behaviours, as well as negligent or reckless ones.

Prior to our final search strategy (outlined below), we performed a series of pilot searches to identify relevant search terms and eligibility criteria to achieve a balance between sensitivity (i.e., retrieving a high proportion of relevant sources) and precision (i.e., retrieving a low proportion of irrelevant articles (Tompson and Belur [42])). We then performed the final search, screened the deduplicated titles and abstracts, screened the full texts, and extracted data from the resulting set of included papers. The search was carried out on 24 July 2024.

2.2. Literature sources

To cast our search net as wide as possible (i.e., covering academic and grey literature from any discipline), we queried the Web of Science (Core Collection), ProQuest Central and IEEE Xplore citation databases. Web of Science is a research search engine that provides access to multidisciplinary, regional and specialist citations. ProQuest Central indexes academic publications, as well as dissertations, working papers from organisations such as National Bureau for Economic Research (NBER) and Organisation for Economic Cooperation and Development (OECD), newspapers and magazines, up-to-date company reports, market and industry reports, and country profiles. The latter grey literature is important, as CCMTs are discussed by many reliable non-academic sources, e.g. the Intergovernmental Panel on Climate Change (IPCC), which are indexed by ProQuest Central. We acknowledge that ProQuest Central mostly indexes non-European grey literature sources and hence is not exhaustive. However, our interest in including grey literature was mainly driven by considering industry and governmental reports written in English (as opposed to covering the full spectrum of grey literature across all possible geographies), we do not consider this a significant limitation. IEEE Xplore is a digital library focused on electronic and electrical engineering and computer science. It provides access to scientific and technical content (including books, conferences, courses, journals, magazines, and standards) published by the IEEE (Institute of Electrical and Electronics Engineers) and its publishing partners.

2.3. Search query

Our search consisted of terms for both CCMTs and crime. For the CCMT terms, we consulted with climate change experts to validate our understanding and categorisation of CCMTs, and to identify the exact terms to use. Instead of searching based on names of specific CCMTs (e.g. “solar panel”, “wind turbine”) which risked neglecting CCMTs that we may be unfamiliar with or do not know the specific search terms for, we employed search terms that pertain to the functional characteristics of CCMTs as described in the introduction. For example, given CCMTs’ objective to reduce carbon emissions, we used terms like “decarboni*” (where the syntax ”*” is a wildcard to represent all words that start with the word fragment specified, e.g. decarbonise and decarbonisation) and “negative emission*”. Similarly, instead of listing every possible renewable or clean energy source, we used “renewable energ*” and “green energ*”. To account for broader technological advances, we also added “technology” terms like “devic*”, “software” and “hardware” to the final search query.

The crime-related terms reflect the broad definition of (future) “crime” as described above and those used in similar scoping reviews on future crimes facilitated by new technologies (e.g., Gomez-Quintero et al. [22]). These include more general terms such as “violen*”, “offen*” and “misus*”. We also used a proximity operator for the terms “threat” and “risk” to be NEAR “security” or “harm*”, to control for the otherwise large number of irrelevant papers that mention the “threat of climate change”, but did not mention any criminal risk. Following recommendations from the climate change experts consulted, we also included specific crime/criminogenic terms such as “money launder*”, “greenwash*” and “theft”, as these crime risks are widely expected in relation to certain CCMTs.

For Web of Science and ProQuest Central, the query below was used to search the ABSTRACT, TITLE and AUTHOR KEYWORDS of each database:

1. (“technol*” OR “devic*” OR “machin*” OR “equipment” OR “apparatus” OR “computer” OR “software” OR “hardware” OR “artificial intelligence”) *AND*
2. ((“mitigation technol*” NEAR/10 climate) OR “decarboni*” OR “greenhouse gas reduc*” OR “carbon reduc*” OR “carbon abatement” OR “carbon stor*” OR “carbon capture” OR “carbon sequestration” OR “carbon utili*” OR “negative emission*” OR “clean energ*” OR “green energ*” OR “renewable energ*” OR “nuclear energy” OR “nuclear power” OR “energy efficiency” OR “nuclear fusion”) *AND*
3. (crim* OR fraud* OR scam* OR corrupt* OR brib* OR hack* OR attack* OR cyberattack* OR cybercrim* OR theft OR steal* OR embezzle* OR misappropriat* OR greenwash* OR “money launder*” OR abus* OR misus* OR offen* OR “tax evasion” OR “tax avoidance” OR violen* OR traffic* OR terror* OR vulnerab* OR threat NEAR/10 (security OR harm*) OR risk NEAR/10 (security OR harm*)) *AND*
4. (“climate change” OR “global warming”)

For IEEE Xplore, we used a broader query because of the limitations imposed by the IEEE search interface (i.e., a maximum 25 keywords and 9 wildcards per query, and a non-functional NEAR operator). In this case, we used the ALL METADATA field to search for:

1. (mitigat* OR carbon OR energ* OR nuclear OR emission) AND
2. (crim* OR corrupt* OR threat NEAR/3 secur* OR greenwashing OR misappropriate OR theft OR embezzle* OR launder OR abus* OR misu* OR offen* OR tax evasion OR tax avoidance OR terroris*) AND (“climate change” OR “global warming” OR “greenhouse gas”)

2.4. Inclusion and exclusion criteria

Only studies that discussed both crime or security threats and/or potential countermeasures and CCMT(s) were included. Other inclusion and exclusion criteria are specified below: *Inclusion criteria:*

1. Papers must discuss one or more CCMTs, and crime or security threats or any other relevant social harm* facilitated or enabled by such technologies and/or relevant countermeasures;
2. Academic and non-academic publications, including (non-)peer-reviewed, book chapters/excerpts, industry reports, newspaper and magazine articles, opinion pieces, and patents;
3. Studies from any discipline;
4. Studies or reports employing any type of research method or design (i.e., qualitative and quantitative, including systematic reviews and meta-analyses, randomised controlled trials, cohort studies, case-control studies, cross-sectional surveys, case reports, position papers, book chapters).
5. Studies published at any point in time.

Exclusion criteria:

1. Social media posts, blogs, and websites;
2. Art and aesthetic works, audio and video transcripts, podcasts, “other sources” (as indexed by ProQuest Central);
3. Duplicate sources;
4. Sources that do not address any crime, safety (i.e, non-malicious, accidental risks) or security risk or threat;
5. Sources concerning climate change adaptation technologies or other non-mitigation technologies.

2.5. Inter-rater reliability and agreement

Two authors independently screened the titles and abstracts of 10% of the identified papers to assess whether they met the inclusion criteria, using an online collaborative literature review interface (Rayyan.ai). Inter-rater reliability (IRR) was assessed based on two coding categories (i.e. inclusion versus exclusion) on the 10% subset, using the prevalence- and bias-adjusted kappa (PABAK) statistic, which controls for chance agreement (Byrt [43]; Byrt et al. [44]). The following cut-offs were used to assess IRR: 0.40–0.59 indicates fair agreement, 0.60–0.74 indicates good agreement and ≥ 0.75 indicates high agreement. Once an adequate IRR score of at least 0.75 was achieved on the random subset, the first author screened the remainder of the papers.

We did not have any major disagreements on what articles to in- or exclude, as the objectives of this review, as well as the inclusion/exclusion criteria, were thoroughly discussed and agreed upon by the authors before finalising this protocol. Any doubts on inclusion/exclusion of specific papers were resolved through informal conversations guided by the eligibility criteria set out by the review protocol.

2.6. Data extraction

Once all titles and abstracts were screened, the first author screened the full texts against the inclusion/exclusion criteria and extracted the following qualitative data from the remaining articles:

1. Type(s) of CCMT discussed;
2. Summary of the intended function of the CCMT;
3. Crime threat(s) mentioned or discussed;
4. Synopsis of the described crime threat and its scenarios;
5. Countermeasure(s) mentioned or discussed;
6. Methods adopted—if empirical (i.e., the paper involves first-hand experiment data/systematised observations, not a speculation/legal analysis), a synopsis of what method(s) were used to obtain the results.

2.7. Thematic analysis

We used constructivist thematic analysis to synthesise the results (Braun and Clarke [45]). This approach has been particularly helpful in the context of identifying future crime threats related to emerging technologies, given the complex nature of the topic and the heterogeneity of articles reviewed (Gomez-Quintero et al. [22]). The results were grouped by themes and subthemes, where themes represent broad categories of crime threats (e.g. property offences) or countermeasures (e.g. technological measures) of a common nature. Subthemes conceptualise more specific groups or types of crime threats (e.g. theft, vandalism) or countermeasures (e.g. cybersecurity measures) that we identify within their broader category. We refined the themes and subthemes through multiple discussion rounds (amongst the authors) until consensus was reached. For each crime threat, we also extracted examples of possible scenarios in which the threat could manifest or modus operandi discussed in the literature. To make the findings of the study relevant for law- and policymaking, we aimed to align the themes and subthemes with familiar legal terminology. For example, we chose to use the term "computer misuse" to define one of the crime themes instead of "cybersecurity threats" to identify behaviours that fit the offences defined by the UK Computer Misuse Act 1990.

2.8. Ethics

This study was approved by the departmental research ethics committee. The publication of this review may enhance and disseminate knowledge on how CCMTs could be misused. Any such adverse effect was pre-empted by briefing relevant stakeholders (e.g. government officials and policymakers) before publication to make them aware of the identified threats and possible countermeasures.

3. Results

As shown in Fig. 1, our final search query yielded a total of 1139 unique papers. Of these, 97 ultimately met our inclusion criteria. In the next sections, we first describe the crime threats identified across these articles and then the identified countermeasures.

3.1. Crime threat scenarios

The thematic analysis revealed 20 distinct crime threats that we clustered in the following six broader categories: 1. property offences; 2. cyber-attacks; 3. financial crime and corruption; 4. environmental threats; 5. human rights abuse; and, 6. national security threats. The first two categories concern crime threats that target CCMTs. The following three categories (3–5) concern threats that are enabled or facilitated by CCMTs, their development, or their operational context. The sixth category includes both kinds of threats. Many articles tended to mention more than one crime threat or multiple possible scenarios of the same threat. The thematic conceptualisation of the threats and their clustering into broader categories required considerable reflection and discussion, firstly, because not all the papers explicitly discussed such threats as criminal offences, secondly, because not all these threats are already criminalised in various jurisdictions, and finally, because there are many possible ways to conceptualise crime threats and group them. We chose to adopt as a main criterion to differentiate between threats and their categories the conduct or modus operandi of the perpetrators rather than the harms caused. For instance, stealing, destroying or fraudulently appropriating a CCMT are different behaviours that might cause a similar loss to the victim. This allowed us also to align our analysis with established definitions of criminal offences across different jurisdictions (e.g. theft, criminal damage, fraud etc.), which was also helpful to identify threats that might not be criminalised yet, despite sharing similar elements with existing offences.

We found that the 97 included articles discussed CCMTs of one of three functional types: renewable energies and their infrastructural systems (e.g. smart grids, wind turbines, solar panels), carbon capture, utilisation and sequestration (CCUS; e.g. atmospheric carbon capture, geological carbon sequestration), or electric vehicles (e.g. electric cars, electric scooters). We then counted how many included references mentioned specific crime threats in relation to one of these three CCMT categories. These relations are depicted in Fig. 2, and the exact counts and references are given in Table 1. Below, we describe each category, its specific crime threats, and examples of scenarios identified in the literature.

3.1.1. Property offences

Several papers discussed two main threats concerning property offences against CCMTs and related infrastructure: (i) theft and (ii) criminal damage. Of these, ten articles linked a property offence to a renewable energy system, 6 articles linked such a scenario to electric vehicles and one article linked a property offence to CCUS. Scenarios of theft included the theft of electric vehicles (Isik et al. [71]; Vaidya and Mouftah [70]; Raj et al. [74]), theft of batteries (Sivasankaran and Jebaraj [138]) and the theft of energy (Merlin et al. [139]; Boamah [122]). One article detailed how criminals could steal energy from charging points, which requires technical knowledge on physically changing electric currents, and clever tampering with coils and wires in such charging systems (Zheng [137]). There were also suggestions of vandalism against "clean cooking" equipment installed in rural colleges in Uganda that were intended to facilitate a transition to a low-carbon lifestyle. Such attacks were believed to be motivated by conflicts of interest, in particular, by some college students who had an additional source of income selling charcoal to the college (Limpens et al. [136]). These findings reveal how climate technologies can enable motivations

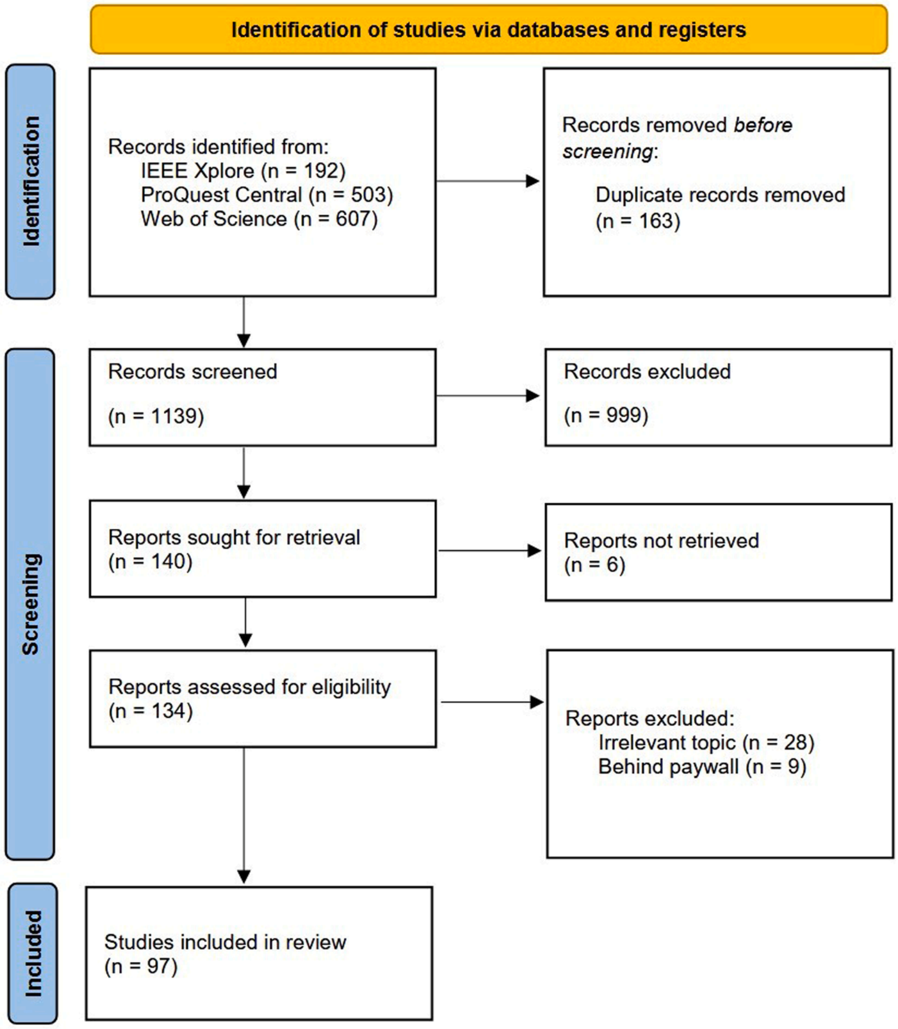

Fig. 1. PRISMA flow diagram, adapted from Page et al. [36].

and opportunities for new ways of perpetrating well-known offences.

3.1.2. *Cyber-attacks*

Of the 97 articles included in this review, 40 discussed malicious uses of computer or network components in a CCMT of which 26 mentions were linked to a renewable energy technology, 13 were linked to electric vehicles and 1 linked to CCUS. These were grouped into a broad cyber-attacks category, which includes two main threats: (i) the hacking or misuse of the computing or networking components of CCMTs to steal, intercept or tamper with (sensitive) data or software that are stored or running on them, respectively; (ii) the hacking or misuse of such systems to enable other offences. Scenarios of the former threat included cyber-attacks on smart energy grids or charging points to breach and manipulate user and usage data (Faheem and Al-Khasawneh [83]; Isik et al. [71]; Vaidya and Mouftah [70]; Attanasio et al. [60]), cyber-attacks by disgruntled employees, or cyberattacks conducted to unlawfully access competitors' data and intellectual property (i.e., industrial espionage) (Ahmed [93]; Greiman [84]). Scenarios of the latter threat include cyber-attacks on smart grids to cause power outages (blackouts) and inconvenience in remote areas with few charging points (Yazdanipour et al. [92]; Dorji et al. [102]; Pourmirza and Walker [95]; Aziz et al. [89]); the hacking of battery systems to cause physical (property) damage (Rahman et al. [66]; Sivasankaran and Jebaraj [138]; Tabuchi and Plumer [77]); the hacking of ride-sharing apps (the use of which reduces emissions by reducing the need for cars) to enable largescale theft of electric vehicles (Vaidya and Mouftah [70]); cyber-attacks intended to prevent people from using digital platforms for renting e-scooters (Isik et al. [71]); tampering with charging points to draw more energy than paid for, e.g., by launching an impersonation attack to charge other users for the energy obtained by the attacker (Attanasio et al. [60]); and exploiting vulnerabilities in the electronic carbon market registration system to commit cyber theft and financial scams (McKie et al. [26]).

3.1.3. *Financial crime and corruption*

Thirty-three articles discussed financial crime or corrupt behaviours. Of these, 23 articles mentioned a financial crime or corruption scenario in conjunction with renewable energy system, six articles mentioned such threats in relation to CCUS projects, and four articles linked a financial crime or corruption scenario to electric vehicles. The specific crime threats within this category were (i) tax fraud and avoidance; (ii) corrupt practices related to the funding and development of CCMT-related projects; (iii) "greenwashing"; (iv) carbon market abuse and manipulation (e.g. monopolies, unfair competition and other market power abuses); (v) carbon credit-based money laundering; and (vi) carbon credit frauds. We considered carbon credit-related threats within scope, since carbon credit markets are often closely related to CCUS initiatives. Below, we synthesise some of the scenarios discussed in the literature for each of these threats.

For tax fraud and avoidance, we found reports of the large-scale carbon credit VAT fraud in the 2010s which involved the purchase of carbon credits in low-tax countries and the selling of them in high-tax

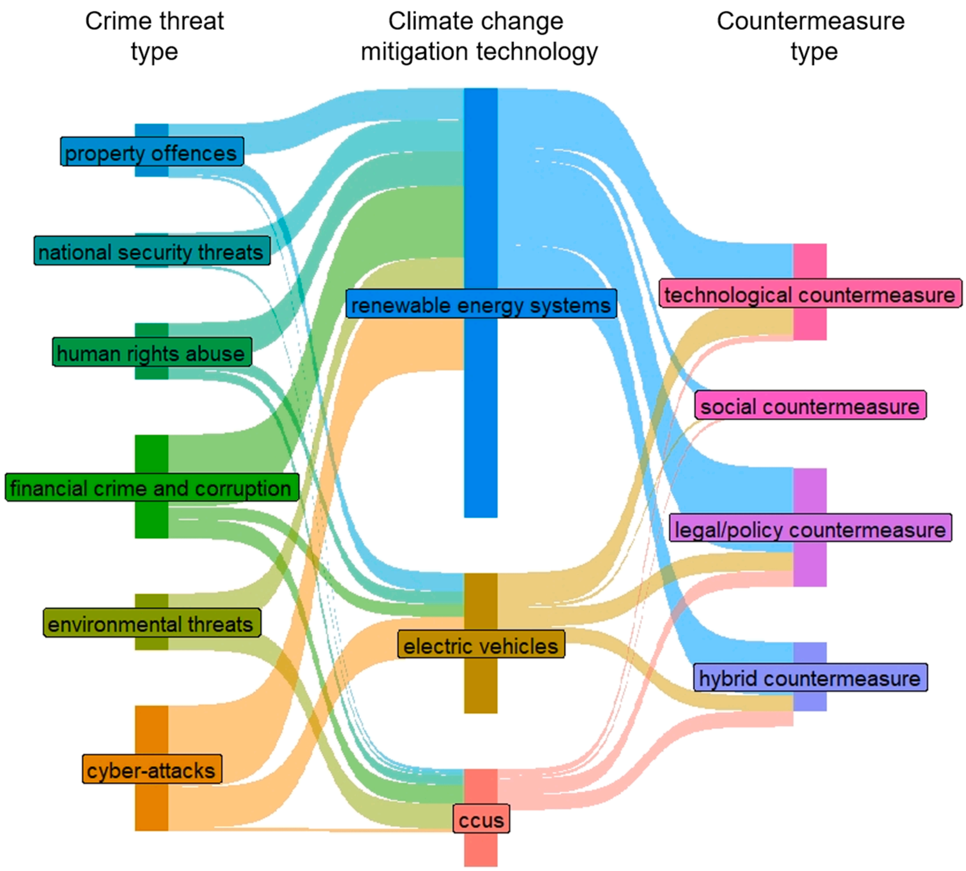

Fig. 2. Overview of the identified crime threat and countermeasure types in relation to three climate change mitigation technology (CCMT) categories. Width of the coloured bands indicates the number of references in which the depicted link was found i.e., the wider the band, the more papers discussed the indicated relationship. See Tables 1 and 2 for the exact frequencies and references.

countries without paying the difference to the states involved (McKie et al. [26]; Williams [25]), the potential abuse of the CCUS tax credit system to avoid tax (Bacci [56]), and tax avoidance by businesses that inflate their (green) innovation input costs to obtain tax relief (Liu et al. [112]). Corrupt practices ranged from the inappropriate allocation and wastage of resources (time, money, materials) that can compromise sustainable development projects and the quality of renewable energy infrastructure (Kwakwa [108]; Jepng'etich [115]; Boamah [122]), to corrupt political networks in developing countries that support dependency on fossil fuels or otherwise halt sustainable developments (Hamann et al. [114]), and rent-seeking, which involves the acquisition of subsidies for sustainable development projects without the delivery of them (Chirambo [105]; Liu et al. [112]).

Articles that mentioned greenwashing cases suggest that corporations may invest in the voluntary carbon market to create the illusion of ecological welfare to the public and other stakeholders (e.g. shareholders) (McKie et al. [26]). Companies may also invest in CCUS technology and carbon markets to distract the public from any adverse impact of their business on the climate and even use it to justify “business as usual”— such as a reliance on unsustainable production processes (Hughes et al. [119]; Sadawi et al. [54]). One article also noted that nuclear power can be misrepresented as clean energy (Pop [117]), although this may depend on how radioactive waste is managed. Organisations may also underestimate greenhouse gas emissions and overestimate future greenhouse gas reductions, either intentionally or unintentionally, since there is no universally agreed way of measuring carbon emissions (Pfadt-Trilling and Fortier [116]). Due to the same inconsistency in or lack of standardised emission measurement tools, estimations of carbon allowances traded on carbon markets may also be easily manipulated by traders (Sadawi et al. [54]; Thirunavukkarasu et al. [57]). Manipulation of the voluntary carbon market could also be facilitated by a lack of transparency, corruption and complexity in the process of allocating carbon allowances (Sadawi et al. [54]), and local energy markets may face unfair competition due to monopolistic tendencies of established electricity distributors/suppliers (Boamah [122]). As for money laundering, Interpol previously reported on large-scale opportunities for buying carbon credits with “dirty” money which creates a “layer” of legitimacy that makes the proceeds of crime harder to trace (Williams [25]; McKie et al. [26]). Finally, scenarios of carbon credit fraud include selling false, unsubstantiated carbon credits, and the making and selling of fraudulent carbon offset certificates, which is further facilitated by laissez-faire environments and poor government controls in carbon and green credit markets (McKie et al. [26]).

3.1.4. *Environmental threats*

Eighteen articles discussed crime threats that would harm the environment. Such threats are: (i) harm to (protected) ecological life from renewable energy development; (ii) environmental threats from CCUS projects; (iii) environmental threats from mining activity; (iv) harms related to nuclear energy; and (v) water insecurity. Scenarios of the first two threats include creating offshore wind farms in or near to marine protected areas that harm ecological life and sea views (Lloret et al. [129]; Soria-Rodriguez [130]), the unintentional killing of protected bird species that fly into wind turbines—which is a criminal offence in the US (Ferrey [128]); groundwater and soil contamination, open water acidification or increases in toxic metals caused by carbon dioxide leaks as a result of carbon sequestration processes (Eldardiry and Habib [48]; Almagro-Pastor et al. [46]; Rojas-Rueda et al. [53]), and increased nitrogen oxide (i.e., another important greenhouse gas) emissions caused by adding carbon capture processes in power plants (Climate Justice

Table 1
Overview of the number of references that describe a climate change mitigation technologies (CCMTs) linked to a specific crime threat type and the identified references.

tech	threat	count	references
carbon capture and sequestration (CCUS)	environmental threats	8	Almagro-Pastor et al. [46]; Byers et al. [47]; Eldardiry and Habib [48]; Merschmann et al. [49]; Rosa et al. [50]; Climate Justice Alliance [51]; Sovacool et al. [52]; Rojas-Rueda et al. [53]
	financial crime and corruption	6	McKie et al. [26]; Sadawi et al. [54]; Du et al. [55]; Bacci [56]; Thirunavukkarasu et al. [57]; Climate Justice Alliance [51]
	human rights abuse	3	Davidson et al. [58]; Rojas-Rueda et al. [53]; Jaschke and Biermann [59]
	cyber-attacks	1	McKie et al. [26]
	national security threats	1	Sovacool et al. [52]
	property offences	1	Sovacool et al. [52]
electric vehicles	cyber-attacks	13	Attanasio et al. [60]; Kumar et al. [61]; Jang et al. [62]; Eghtessad et al. [63]; Cleveland [64]; Beheshteh et al. [65]; Rahman et al. [66]; Wang et al. [67]; Yuan and Li [68]; Reddy et al. [69]; Vaidya and Mouftah [70]; Isik et al. [71]; Tembo and Nyoni [72]
	property offences	6	Reddy et al. [69]; Vaidya and Mouftah [70]; Isik et al. [71]; Patel and Roscia [73]; Tembo and Nyoni [72]; Raj et al. [74]
	financial crime and corruption	4	Badhwar and Galodha [75]; Tembo and Nyoni [72]; Patel and Roscia [73]; Sovacool [76]
	human rights abuse	4	Badhwar and Galodha [75]; Tabuchi and Plumer [77]; Huber and Steininger [78]; Sovacool [76]
renewable energy systems	cyber-attacks	26	Elsayed et al. [79]; Allal et al. [80]; Asif et al. [81]; Cali et al. [82]; Faheem and Al-Khasawneh [83]; Greiman [84]; Ahmed et al. [85]; Mishra et al. [86]; Živic et al. [87]; Rekeraho et al. [88]; Aziz et al. [89]; Chakraborty et al. [90]; Pareek et al. [91]; Yazdanipour et al. [92]; Ahmed [93]; Chen and Ko [94]; Pourmirza and Walker [95]; Zhang et al. [96]; Yuan and Li [68]; Sayali et al. [97]; Kivimaa et al. [98]; Zhang et al. [99]; Falowo et al. [100]; Gambhir and Lempert [101]; Dorji et al. [102]; Tembo and Nyoni [72]
	financial crime and corruption	23	Sayali et al. [97]; Ali et al. [103]; Chen et al. [104]; Chirambo [105]; Engelken et al. [106]; Khan and Hassan [107]; Kwakwa [108]; Kivyiro and Arminen [109]; Ren et al. [110]; Shahnazi and Alimohammadlou [111]; Liu et al. [112]; Acheampong et al. [113]; Hamann et al. [114]; Jepng'etich [115]; Tembo and Nyoni [72]; Pfadt-Trilling and Fortier [116]; Pop [117]; Vlachou and Pantelias [118]; Hughes et al. [119]; Andreucci and Zografos [120]; Kiehbadroudinezhad et al. [121]; Sovacool [76]; Boamah [122]
	human rights abuse	11	Kivimaa et al. [98]; McKie [39]; Davidson et al. [58]; South African Institute of Chartered Accountants [123]; Copley [124]; Nsafon et al. [125]; Huber and Steininger [78]; Sovacool [76]; Andreucci and Zografos [120]; Dunlap et al. [126]; Hughes et al. [119]
	environmental threats	10	Charles Rajesh Kumar et al. [127]; Ferrey [128]; Lloret et al. [129]; Soria-Rodriguez [130]; McKie [39]; Andreucci and Zografos [120]; Dunlap et al. [126]; BBC News [15]; Hughes et al. [119]; Sovacool et al. [52]
	national security threats	10	Dautray et al. [131]; Jain [132]; Schmid [133]; Sertyesilisik and Melaine [134]; Falowo et al. [100]; Gambhir and Lempert [101]; Dorji et al. [102]; Sovacool et al. [52]; Duffey et al. [135]; BBC News [15]
	property offences	10	Sertyesilisik and Melaine [134]; Zhang et al. [99]; Dorji et al. [102]; Limpens et al. [136]; Sovacool et al. [52]; Tembo and Nyoni [72]; Zheng [137]; Sivasankaran and Jebaraj [138]; Merlin et al. [139]; Boamah [122]

Alliance [51]).

Scenarios of environmental threats from mining activity include direct environmental damage from opening uranium mines required for the development of nuclear power (McKie [39]), harmful air pollution from cobalt mining needed for the development of electric devices/vehicles (Tabuchi and Plumer [77]), and general inappropriate or unlawful exploitation of natural resources in the mining sector (Dunlap et al. [126]; Andreucci and Zografos [120]; Badhwar and Galodha [75]). As for harms related to nuclear energy, a news report noted safety concerns around the risk of accidents or targeted attacks on radioactive waste and nuclear reactors (BBC News [15]) that would lead to severe environmental damage, as well as national security threats (see below). Finally, carbon capture and sequestration installations impose new water stresses due to the additional water requirements for the chemical and physical processes required to capture and separate carbon dioxide. This demand for freshwater has been described as a "parasitic load" that, in fact, reduces the efficiency of power plants where CCUS could be applied (Eldardiry and Habib [48]). Although using large amounts of water is not a crime, many scholarly studies and governmental reports have been concerned about water (in)security. An incessant demand for freshwater could become criminalised if it threatens the livelihood of local communities and other species. In total, eight papers mentioned either of these environmental threats in relation to CCUS projects, and ten articles related them to a renewable energy system (see Table 1).

The overall analysis of these threats suggests that while some of these may be considered closer to what the IPCC defines as anticipated and manageable "trade-offs" between climate action and sustainable development (IPCC [32]), other threats appear to be much more unpredictable and nefarious unintended consequences that require more specific interventions beyond climate policies. This distinction also bears on the seriousness of the threat and on the need for and design of specific laws to criminalise these practices. Harm to ecological life and landscape, for instance, may be a negligent or reckless side-effect of the operation of certain technologies, while the deliberate abuse of natural resources by organised criminal groups or ruthless investors can hardly be considered a "trade-off" as it is a much more problematic unintended consequence.

3.1.5. Human rights abuse

Eighteen articles discussed human rights abuses involved in the development of CCMTs, of which 11 linked a form of human rights abuse to renewable energy systems, 4 articles related it to electric vehicles, and three articles related human rights abuse cases to CCUS. Threats in this category consisted of: (i) slavery, forced and illegal labour (including child labour), and (ii) dispossession of land and displacement of people. Various articles described cases of children working in mining sites essential for the development of various CCMTs (Nsafon et al. [125]; Kivimaa et al. [98]; Badhwar and Galodha [75]; Huber and Steininger [78]), the mistreatment of female workers and minority communities in India involved in the supply chain of electric vehicles (Badhwar and Galodha [75]), and widespread human trafficking and forced labour in mining sites, and solar panel and low-carbon technology factories (Copley [124]; Huber and Steininger [78]; Davidson et al. [58]; Sovacool [76]).

The dispossession of land from indigenous communities ('land grabbing' and through land enclosures) and the displacement of people from these communities are often discussed with other socioecological harms such as the intensive exploitation of local natural resources and unfair practices from international investors, usually in countries in the Global South, to facilitate the development of CCMTs (Dunlap et al. [126]; Rojas-Rueda et al. [53]; Jaschke and Biermann [59]; Sovacool [76]; Andreucci and Zografos [120]). Some papers go as far as to suggest that the development of environmental infrastructures can be a mechanism to justify the appropriation and dispossession of land as part of broader patterns of domination, "extractivism" and neocolonialism (Hughes et al. [119]; Andreucci and Zografos [120]). Thus, these are not only instances of land dispossession, but greenwashing too (see above).

Together, these papers show how CCMTs can facilitate threats to core values and principles of the broader notion of "human security" (cf. Malmio [33] and Salas Alfaro et al. [10]), such as individual rights, justice and access to natural resources, which are also embedded in several SDGs. This also highlights how some threats enabled by CCMTs are not mere trade-offs, but much more complex and serious security problems.

3.1.6. National security threats

Eleven articles considered three crime threats related to national security–that is, a narrower and more state-focused definition of security than "human security": (i) terrorism; (ii) territorial conflict; and (iii) geopolitical blackmail. Of these, 10 articles mentioned them in conjunction with a renewable energy system, and one article linked it to CCUS. Scenarios of terrorist threats mostly concern "nuclear terrorism", such as building or getting a hold of nuclear weapons, attacks on nuclear facilities or nuclear materials in transit, or suicide attacks using radioactive material (Dautray et al. [131]; Falowo et al. [100]; BBC News [15]; Duffey et al. [135]; Schmid [133]; Jain [132]). Territorial conflict may come from disagreements between states over whether to use certain marine spaces for offshore wind farms and ocean energy installations, especially in marine areas beyond national jurisdictions (Soria-Rodriguez [130]). Scenarios of geopolitical blackmail are discussed in a study in which policymakers were interviewed about their perceived security risks related to climate change. According to some respondents, rogue states, terrorists, and other malicious actors could threaten to suspend the operation of climate systems or even release carbon from their reservoirs, unless "their demands were met" (Sovacool et al. [52]). Although conflicts are not inherently criminal despite the harm they can involve, these latter scenarios imply how conflicts over CCMT implementations can lead to crime threats. In any case, the emergence of asymmetric and hybrid warfare has somewhat blurred the boundary between what is criminal and what is war-related.

3.2. Countermeasures

Through thematic analysis, we identified 22 distinct types of countermeasures, which we grouped into four pre-defined categories: (i) technological measures, (ii) legal/policy measures, (iii) social measures, and (iv) other/hybrid measures. Not all articles mentioned a countermeasure, hence the total number of articles referenced here is lower than 97. The thematic identification of countermeasures and related categories inevitably followed a different analytical process than that used for crime threats. The guiding principle here was the nature of the countermeasure (e.g. technological or regulatory or hybrid) and the actors responsible for its implementation (e.g. technology researchers and developers, industry actors, policymakers or lawmakers). The choice of adopting quite a high-level quadripartite categorisation was dictated by the diverse nature of many threats we identified, which would have made a more nuanced categorisation more challenging. As with the crime threats, we counted the number of references in which a countermeasure type was described in relation to one of the three functional CCMT categories present in the included set of 97 articles; see Fig. 2 and Table 2.

Overall, the countermeasures analysis suggests that the effective prevention and reduction of the identified crime threats requires the mobilisation of many different stakeholders, especially when CCMTs rely on a complex integration of different technologies. Some of the crime risks may be already addressed by policies, regulations and practices that govern those components. For instance, unlawful or exploitative labour practices can be addressed by existing legal frameworks to protect workers' rights. Likewise, threats enabled by specific technological components of CCMTs such as computer systems can be addressed by cybersecurity measures and laws. Other risks, however, cannot be mitigated purely through existing frameworks and require specific new interventions. For instance, specific technological devices or measures might be required to address specific risks enabled by new technologies or new criminal laws might be required to criminalise threats that are not yet defined by the law as criminal offences.

3.2.1. Technological measures

Thirty-one articles mentioned at least one technological countermeasure, of which 19 mentioned a technological countermeasure in relation to a renewable energy system, 10 articles in relation to electric vehicles, and two articles in relation to CCUS. We divided these into four main types: (i) cybersecurity measures; (ii) decentralisation of energy systems; (iii) physical security measures; and (iv) carbon tracking methods. Cybersecurity measures include anti-location-spoofing mechanisms through multiple methods to validate an electric vehicle's location (Isik et al. [71]), anomaly detection systems to detect tampering with electric vehicles and the power infrastructure (Cali et al. [82]; Rahman et al. [66]; Merlin et al. [139]; Faheem and Al-Khasawneh [83]), firewalls (Chen and Ko [94]), encrypting data (Ahmed [93]; Jang et al. [62]; Rekeraho et al. [88]; Isik et al. [71]), using federated learning for privacy-preserving machine learning model development (Wang et al. [67]), vulnerability simulations (Sayali et al. [97]), biometric access control to prevent theft of electric vehicles (Raj et al. [74]) and other stronger authentication systems for users of smart grid charging systems (e.g. token-based authentication) (Vaidya and Mouftah [70]), using blockchain technology to track energy sources on smart grids (Ahmed et al. [85]), developing machine learning models based on behavioural energy usage data to detect energy theft (Zheng [137]), and methods to detect and prevent false data injection in power system operators that would otherwise cause errors in energy charges and power supply issues (Elsayed et al. [79]). The second type of technological countermeasure involves the decentralised design of energy systems to minimise the risk and impact of any potential incidents in

Table 2
Overview of the number of references that describe climate change mitigation technologies (CCMTs) linked to a specific countermeasure type and the corresponding references.

tech	countermeasure type	count	references
carbon capture and sequestration (CCUS)	hybrid countermeasure	5	Byers et al. [47]; Eldardiry and Habib [48]; Climate Justice Alliance [51]; Rojas-Rueda et al. [53]; Du et al. [55]
	legal/policy countermeasure	5	Rojas-Rueda et al. [53]; Bacci [56]; Davidson et al. [58]; Jaschke and Biermann [59]
	technological countermeasure	2	Sadawi et al. [54]; Thirunavukkarasu et al. [57]
	social countermeasure	1	Rojas-Rueda et al. [53]
electric vehicles	technological countermeasure	10	Attanasio et al. [60]; Kumar et al. [61]; Jang et al. [62]; Eghtessad et al. [63]; Rahman et al. [66]; Wang et al. [67]; Reddy et al. [69]; Vaidya and Mouftah [70]; Isik et al. [71]; Raj et al. [74]
	legal/policy countermeasure	6	Kumar et al. [61]; Isik et al. [71]; Badhwar and Galodha [75]; Patel and Roscia [73]; Sovacool [76]; Huber and Steininger [78]
	hybrid countermeasure	5	Kumar et al. [61]; Cleveland [64]; Beheshteh et al. [65]; Yuan and Li [68]; Huber and Steininger [78]
	social countermeasure	1	Kumar et al. [61]
renewable energy systems	legal/policy countermeasure	27	Asif et al. [81]; Pareek et al. [91]; Kivimaa et al. [98]; Charles Rajesh Kumar et al. [127]; Ferrey [128]; Lloret et al. [129]; Soria-Rodriguez [130]; McKie [39]; BBC News [15]; Ali et al. [103]; Chen et al. [104]; Khan and Hassan [107]; Kwakwa [108]; Kivyiro and Arminen [109]; Shahnazi and Alimohammadlou [111]; Acheampong et al. [113]; Jepng'etich [115]; Sovacool [76]; Boamah [122]; Davidson et al. [58]; Copley [124]; Nsafon et al. [125]; Huber and Steininger [78]; Dautray et al. [131]; Schmid [133]; Sertyesilisik and Melaine [134]; Duffey et al. [135]
	technological countermeasure	19	Elsayed et al. [79]; Allal et al. [80]; Cali et al. [82]; Greiman [84]; Ahmed et al. [85]; Mishra et al. [86]; Zivic et al. [87]; Rekeraho et al. [88]; Aziz et al. [89]; Ahmed [93]; Chen and Ko [94]; Pourmirza and Walker [95]; Zhang et al. [96]; Sayali et al. [97]; Zhang et al. [99]; Kiehbadroudinezhad et al. [121]; Zheng [137]; Sivasankaran and Jebaraj [138]; Merlin et al. [139]
	hybrid countermeasure	17	Faheem and Al-Khasawneh [83]; Greiman [84]; Aziz et al. [89]; Chakraborty et al. [90]; Yazdanipour et al. [92]; Chen and Ko [94]; Yuan and Li [68]; Sayali et al. [97]; Kivimaa et al. [98]; Falowo et al. [100]; Gambhir and Lempert [101]; Dorji et al. [102]; Chirambo [105]; Kivyiro and Arminen [109]; Ren et al. [110]; Liu et al. [112]; Huber and Steininger [78]
	social countermeasure	5	Asif et al. [81]; Pareek et al. [91]; Falowo et al. [100]; Greiman [84]; Vlachou and Pantelias [118]

(smart) energy grids. For example, "microgrid islanding" allows eco-friendly systems to operate independently during emergencies or grid disruptions, thus ensuring a continuous power supply to critical loads (Kiehbadroudinezhad et al. [121]). The third set of technological countermeasures involves physical situational measures to increase the effort required to commit offences related to CCMTs such as theft or criminal damage, or increase the risk of detection. Examples of these measures include surveillance cameras (Sayali et al. [97]), physical/-wheel locks (Isik et al. [71]) and battery theft detection model (Sivasankaran and Jebaraj [138]). The fourth set considers using blockchain technology to track carbon credits and energy sources when using smart (energy) grids (Sadawi et al. [54]; Ahmed et al. [85]), which would improve the transparency of where carbon offsets and energy on grids come from.

3.2.2. *Legal/policy measures*

Thirty-eight articles mentioned legal or policy countermeasures, of which 27 were linked to renewable energy systems, 6 related to electric vehicles and 5 to CCUS. This category includes 11 different types of countermeasures: (I) policies to improve the fairness and integrity of the carbon and energy markets, including market power assessments (Du et al. [55]), and measures to prevent monopolies such as reducing the segmentation of the energy market, promoting the internal opening of the energy market, breaking the monopoly of ownership and strengthening supervision to reduce rent-seeking of local governments and state-owned enterprises, reducing governmental interventions in energy prices to promote market flow, and achieving equal competition between private enterprises (Ren et al. [110]); (II) development and enforcement of environmental laws to protect local ecosystems and protected species from disruption caused by CCMT development, such as establishing community-based institutions for the management of local natural resources (e.g. Community Forest Associations in Kenya) and giving local communities property rights over such resources (e.g. trees) (Jepng'etich [115]), as well as policies and laws to exclude marine protected areas with high biodiversity and sensitive or threatened species and habitats from offshore wind farm development (Lloret et al. [129]; Charles Rajesh Kumar et al. [127]); (III) protecting the human rights of individuals involved in supply chains of CCMT, including policies and laws against child or illegal labour (Badhwar and Galodha [75]; Yuan and Li [68]; Kumar et al. [61]) and the sexual harassment of female employees (Badhwar and Galodha [75]); (IV) policies for the security of and equal access to natural resources, such as regulation of appropriate resource extraction methods to reduce the degradation of the environment and carbon emission (Dunlap et al. [126]); (V) policies to ensure that vulnerable and marginalised communities can benefit from the sustainable energy transition (Nsafon et al. [125]), and mitigating the risks of water insecurity through national strategic plans for a future that relies on low levels of nuclear and carbon capture (Byers et al. [47]); (VI) international laws, such as treaties on non-proliferation of nuclear weapons (Duffey et al. [135]), and watchdogs, such as the International Atomic Energy Agency (IAEA; Dautray et al. [131]); (VII) international cooperation, commitment and assurances, such as a partnership among the seven emerging economies ("E-7" countries, i.e., China, Brazil, Indonesia, India, Russia, Turkey, and Mexico) and other partners to share best practices, knowledge, and the transmission of technology (Chen et al. [104]), international pledges by nuclear-armed countries to not be the first to use nuclear weapons in case of a conflict (i.e., "no-first-use") and other "positive security assurance"-type pledges by nuclear-armed states to help those without nuclear weapons if they are ever under nuclear attack (Sertyesilisik and Melaine [134]); (VIII) international sanctions or bans, such as trade or import bans against regions known for systemic or lax prosecution of human rights abuse or with bad labour practices (Copley [124]), or "decoupling" a nation's energy supply from states that represent national security threats (Davidson et al. [58]); (IX) policies and laws to improve institutional quality, good governance and the rule of law, such as anti-corruption frameworks (Chen et al. [104]); (X) national or international legal structures and frameworks to define and prevent tax avoidance, such as the OECD's G20 Base Erosion and Profit Shifting Project (BEPS) (Bacci [56]); (XI) technology and industry regulation, be they voluntary or mandatory, suggested safety and security standards concerning the development and operation of CCMTs, such as a security key agreement protocol and security standards defined by the European Smart Meter Alliance (Zivic et al. [87]; Pourmirza and Walker [95]; Isik et al. [71]; Reddy et al. [69]), as well as corporate compliance and Corporate Environmental Responsibility (CER) frameworks (McKie [39]).

3.2.3. Social measures

We found three countermeasures of a purely social nature (i.e., measures that solely rely on some form of social interaction or initiative): (i) more public-private collaboration in the development and operation of CCMTs (Falowo et al. [100]; Greiman [84]; Rojas-Rueda et al. [53]); (ii) awareness-raising, public engagement, providing information and counter-disinformation (Asif et al. [81]; Pareek et al. [91]; Kumar et al. [61]), e.g. to improve public awareness of cybersecurity threats concerning digital technologies for sustainability purposes (Pareek et al. [91]); and (iii) a sociocultural shift to hold and uphold "eco-socialist" values to facilitate environmentally conscious behaviour (Vlachou and Pantelias [118]). In total, five papers mentioned either of these social countermeasures in relation to a renewable energy system, one paper mentioned a social countermeasure in relation to electric vehicles, and one paper in relation to CCUS.

3.2.4. Other/hybrid measures

Countermeasures in this category do not fit any of the previous categories, because they typically involve a combination of measures of different kinds (e.g. technological and social). We found five countermeasure subthemes here: (i) countermeasures to address property threats or offences targeted at national critical infrastructure by establishing a coordinated and unified national response to such threat, e.g. through a Computer Security Incident Response Team (CSIRT) (Falowo et al. [100]); (ii) developing smart grid safety/security assessment and evaluation criteria (Aziz et al. [89]); (iii) open-sourcing data to improve anomaly detection models for smart energy grids (Faheem and Al-Khasawneh [83]); (iv) applying appropriate risk assessment and management procedures (Gambhir and Lempert [101]); and (v) general capacity-building countermeasures, such as further (long-term) research to better understand crime and security risks related to CCMTs (Yazdanipour et al. [92]; Dorji et al. [102]; Eldardiry and Habib [48]; Rojas-Rueda et al. [53]; Yuan and Li [68]; Cleveland [64]). In total, 17 articles related a hybrid countermeasure to a renewable energy system, 5 mentioned a hybrid countermeasure to electric vehicles, and 5 to CCUS (see Table 2).

4. Discussion

Our systemic dependency on fossil fuels to sustain a modern lifestyle is causing existential risks to humanity by dramatically altering temperature and weather patterns (Jones et al. [140]; Welsby et al. [141]). As a result, technological innovations, such as batteries, wind turbines and solar panels, play a key role in mitigating climate change. These technologies can contribute to the achievement of sustainable development goals, but at the same time they can facilitate crime and security risks that can frustrate the principles and objectives of climate action and sustainable development. The present scoping review provides a comprehensive overview of crime threats and criminogenic risks, as well as potential countermeasures, to help researchers and policymakers pre-empt and address the identified threats.

From over 1100 articles, we found 97 relevant publications (8.5%) that address a crime or security threat related to a specific climate change mitigation technology, of which some also describe a countermeasure. Despite the limited number of relevant articles, we found a broad range of crime and security implications, often in the larger supply chain of CCMT developments. They ranged from carbon fraud and corruption, to geopolitical extortion and cyber-attacks on smart grid infrastructure. The low number of relevant articles strongly suggests a blind spot for the crime and security risks related to CCMTs, at least in the (mostly academic) literature. Although some of the CCMTs within our scope are relatively new (e.g. carbon capture and sequestration), many of them are relatively well-established (e.g. renewable energy sources, electric vehicles). It would thus be surprising, and somewhat alarming, if the number of relevant publications we identified is representative of the knowledge on crime and security risks spread across stakeholders in this field. It is unclear from the literature to what extent these risks are successfully addressed in practice and by whom, which may in itself be a symptom of larger systemic issues in the geopolitically driven discussion on climate change. The late discovery and prosecution of large-scale carbon tax fraud nearly twenty years ago (McKie et al. [26]) and well-known human rights abuse in the mining industry do not allow for a particularly encouraging outlook. It is possible that our search strategy led to the exclusion of certain relevant papers, e.g., on a highly specific CCMT. We do not expect this risk to be high, as our thorough screening process resulted in deeming less than 10% of all retrieved papers as relevant. This low signal-to-noise ratio implies that more attention is needed for our subject matter, including for CCMTs not associated with any particular crime or security risk in this review (e.g., hydrogen power and enhanced weathering).

4.1. Relation between crime threats and specific CCMTs

When it comes to the various crime threat categories, the co-occurrence counts of crime threat types and CCMTs suggest that certain threat types have been discussed more often in relation to certain CCMTs (also see Fig. 2). We find that the crime and security risks described in conjunction with electric vehicles (EVs) tend to be cyber-attacks, theft and human rights abuse in their supply chain (e.g., in mining for precious raw materials required for battery technology). Smart energy grids (here, categorised as an example of a renewable energy system) seem more strongly associated with cyber-attacks, property damage and a proneness to national security threats. Solar panels are more specifically related to theft and human rights abuse in their supply chain (e.g. forced and child labour in manufacturing sites). Wind turbines are related to environmental threats (e.g. killing protected birds in the US), territorial conflict in the case of offshore wind farms and, as with solar panels and EVs, human rights abuse in their supply chain. CCUS techniques were mostly described in relation to carbon credit and carbon offset fraud, environmental threats from insecurely sequestered carbon, as well as blackmail or extortion when certain countries could threaten to use their carbon sinks as a medium of exchange. As a whole, the renewable energy sector (i.e., including both solar panels and wind turbines) may be especially related to market power abuse, corruption and rent-seeking. Note, however, that the limited number of publications on these CCMTs and other crime or security risks does not preclude potential other risks related to these and other CCMTs. Although statistical tests to see which of the co-occurrence counts between CCMTs and crime threats or countermeasures significantly stand out are possible, the largely imbalanced and small sample sizes for each group (see Tables 1 and 2) would not allow for a robust interpretation of such results. It is typical for future crime research to not be able to run such quantitative analyses for these reasons, as well as the fact that there are no or very limited data in general regarding crimes or harmful scenarios that may only become criminalised in the future. Accordingly, the results are mostly of a qualitative nature.

These findings corroborate the validity of situational crime prevention research, as they imply that crime threat opportunities tend to be technology-specific and thus warrant crime-specific prevention measures (as opposed to a more general "blanket crime policy" approach) (Johnson [17]; Clarke [142]). In terms of future research, this suggests that a thorough investigation of specific threats and the contexts and events in which they manifest, especially using crime science approaches such as crime scripting, would provide important insights into possible countermeasures.

4.2. Risks that are not criminal (yet)

Interestingly, this review revealed that there may be a wider scope for criminalising environmental threats in the near future. In countries where certain ecological harms are not legally defined as criminal offences (yet), adverse impacts from CCMT developments will remain less visible and problematic to address, especially in the case of the (unintended) effects of CCUS projects. While not necessarily driven by criminal intent, these harms might still be caused by negligence or recklessness, which in many jurisdictions are sufficient to warrant criminal liability. Various studies indicate the risk of acidification of freshwater and soil, depending on where carbon gets sequestered (Eldardiry and Habib [48]; Almagro-Pastor et al. [46]), and the possibility that such carbon will transpire back into the local ecosystem sooner than later (Mortezaei et al. [143]; Bielicki et al. [144]; Rui et al. [145])—rendering geological and marine carbon sequestration largely ineffective and therefore misleading climate mitigation initiatives. Freshwater contamination and demand from CCUS projects, combined with the rapidly growing, incessant demand for freshwater to cool data centres to power artificial intelligence systems (Li et al. [146]) could negatively affect access to and supply of water resources that are essential to support most life on Earth. Moreover, using CCUS as a justification for not fundamentally making production processes more sustainable is not helpful either in the context of mitigating climate change [51]. Indeed, recent forecasting studies suggest that the scale of these harms could be amplified if wide-scale use of CCUS technologies is politically enforced or encouraged to the extent required to offset the expected growth in carbon emissions (Bindl et al. [147]). Although CCUS may not be implemented with the criminal intent to mislead the public, any unintended consequences to the environment from faulty CCUS applications will impact local communities and could thus warrant criminalisation.

Countries without laws against such environmental threats should explore whether to criminalise them, at least when they are driven by negligence or recklessness. In this context, the suggestion by Polly Higgins to introduce a new core crime of "ecocide" in international criminal law to prosecute large-scale environmental threats (Higgins et al. [148]) could be a fitting legal countermeasure, if indeed the collateral damage from large-scale CCUS is to be regarded as a future crime. Similarly, we find that "greenwashing"—corporate practices of misusing or misrepresenting commitments to sustainable development to conceal their contribution to carbon emissions—is not strictly speaking an illegal activity as of now, but could become a regulatory concern in the near future. Not criminalising or, if appropriate offences already exist, not prosecuting malicious and deceptive greenwashing practices with considerable individual, social and environmental threats, could cause nations to fail to reach their sustainable development goals as per the Paris Agreement.

Another criminogenic factor that may lead to future crime is territorial uncertainty over the use and ownership of stretches of land or sea. There have already been reported tensions, for example, between Taiwan and China, where offshore wind farms from either side may be easy targets for sabotage and offensive escalations (Webster and Leung [149]). Further down the line is when "green projects" (e.g. building solar farms) and mine scouting are used to justify land grabbing from local communities, as the included articles indicate this has already happened to Palestinians (Hughes et al. [119]) and many countries in the "global south" (Jaschke and Biermann [59]; Sovacool [76]), and is a looming risk to the people living in northern Portugal (Dunlap et al. [126]). As noted before, such conflict situations can easily give rise to criminal escalations and exploitations, such as vandalism, violence, and terrorism.

4.3. Need for (more) adequate countermeasures

In terms of countermeasures, we mostly found legal or policy measures, ranging from industry standards for cybersecurity implementations and international sanctions, to environmental laws and carbon market regulations, whereas one might at first expect more technological solutions to address technology-related (crime) problems. Such legal/policy measures typically are challenging to implement, as they heavily depend on collaboration between stakeholders, aligning value systems and enforcement thereof, often at the international level in the context of climate change. Some can even be politically controversial due to their inextricable link to conflicting interests and diverging ideologies, which may hinder the development of the necessary consensus, delay adoption and obstruct objective measurement of their effectiveness. All this can compromise the successful and timely implementation of safety and security measures concerning CCMTs. In addition, many of the countermeasures identified, such as "cultivating an eco-socialist society" (Vlachou and Pantelias [118]) and "further research to better understand crime and security risks related to CCMTs" (e.g., (Yazdanipour et al. [92]; Dorji et al. [102]; Eldardiry and Habib [48]) were too vague to be practically implemented, even though they are important for long-term strategic capacity-building. Thus, the identified literature shows the need for scholars to propose clearer and more feasible solutions. We expect this to be a fruitful area for further research and development, with situational prevention methods especially suited to circumvent some of the politically charged narratives around climate change mitigation—e.g., applying safe-by-design principles (Ekblom [150]) to crime-proof further CCMT developments.

5. Conclusion

The results of this scoping review suggest that, as anticipated by crime harvest theory, the rapid diffusion of climate change mitigation technologies is likely to facilitate a broad range of future crime and security threats. At the same time, the small number of relevant academic and non-academic papers identified by our search indicates that our knowledge in this area remains limited. Our analysis suggests that these threats can have detrimental consequences not only for the environment and climate action itself, but also for broader security concerns, including national security, individual rights and social interests, and, ultimately, for sustainable development. Our research also suggests a similarly broad range of potential countermeasures, also drawing on existing policy, technological or social frameworks, that could help anticipate, prevent and respond effectively to such threats.

These findings provide preliminary empirical groundwork for future research and policy development. Future research could proceed in different directions. First, some of the crime and security threats identified by this study require more focused investigation. This concerns new forms of established offences, such as carbon credit frauds, which, are still under-researched by the literature, particularly in crime science. This also concerns emerging threats whose criminal status remains contested, such as certain forms of environmental harm or greenwashing practices that do not yet fall within existing legal definition of criminal offences and therefore warrant further legal, socio-legal and criminological analysis. Threats associated with the operation and functioning of specific technologies might also require additional security-focused technological research. The countermeasures identified in this study also merit focused examination. Technological countermeasures should be assessed for feasibility and effectiveness, while policy and social measures should be analysed in relation to existing policy and legal frameworks and other initiatives. Future research could evaluate which measures are already in place, how effective they are, and what other interventions may be required. Such research could focus on individual national jurisdictions, comparative legal systems or international instruments. For instance, legal research could assess whether existing criminal offences are sufficient to prosecute the identified threats or whether new forms of criminalisation may be necessary. Second, our findings could inform future efforts to assess and compare the threats or countermeasures identified in this study across multiple dimensions, such as the likelihood and severity of threats or the feasibility and effectiveness of countermeasures. Third, this study may contribute to broader theoretical discussions concerning the complex relationships between climate action, security, and sustainable development or, more broadly, sustainability.

In the shorter term, our findings may assist national and international policymakers and lawmakers in balancing the competing interests involved in climate mitigation when developing new policies and legislation. In particular, they might support the adoption of more comprehensive and systemic approaches to climate action that consider not only environmental and sustainability impacts, but also security concerns, including crime-related risks. The findings may also assist industry actors in assessing the risks associated with the design, manufacture and operation of CCMTs and in implementing appropriate mitigation strategies. More broadly, we hope this study will promote greater public awareness and debate regarding the crime and security implications of climate action, ultimately contributing to the development of more holistic, resilient and future-proof analytical, policy and practical frameworks capable of supporting the fulfilment of the goals of sustainable development and climate action in a safe and secure manner.

CRediT authorship contribution statement

Sarah Y. Zheng: Data curation, Formal analysis, Investigation, Methodology, Project administration, Resources, Software, Validation, Visualization, Writing – original draft, Writing – review & editing. **Shane D. Johnson:** Conceptualization, Funding acquisition, Methodology, Resources, Supervision, Writing – review & editing. **Paul Ekblom:** Resources, Writing – review & editing. **Mark A. Maslin:** Resources, Validation, Writing – review & editing. **Hervé Borrion:** Writing – review & editing. **Lauren Young:** Conceptualization, Writing – review & editing. **Manja Nikolovska:** Conceptualization, Writing – review & editing. **Matthew P.J. Ashby:** Conceptualization, Writing – review & editing. **Lorenzo Pasculli:** Conceptualization, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Supervision, Validation, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare no competing interests.

Data availability

All qualitative and numerical data are supplied in the main text (Results section).

References

[1] S. Fawzy, A.I. Osman, J. Doran, D.W. Rooney, Strategies for mitigation of climate change: a review, Environ. Chem. Lett. 18 (2020) 2069–2094.
[2] UN Framework Convention on Climate Change (UNFCCC), Technologies for Adaptation to Climate Change, Climate Change Secretariat (UNFCCC), 2006.
[3] European Environmental Agency (EEA), 2023. What is the difference between adaptation and mitigation? URL: https://www.eea.europa.eu/help/faq/what-is-the-difference-between.
[4] T. Napp, T. Hills, S.M. Soltani, J. Bosch, C. Mazur, A Survey of Key Technological Innovations For the Low-Carbon Economy, Imperial College London, 2017. URL: https://www.imperial.ac.uk/grantham/research/energy-and-low-carbon-futures/next.
[5] J. Coenen, L.M. Glass, L. Sanderink, Two degrees and the SDGs: a network analysis of the interlinkages between transnational climate actions and the Sustainable Development Goals, Sustain. Sci. 17 (2022) 1489–1510, https://doi.org/10.1007/s11625-021-01007-9.
[6] L. Gomez-Echeverri, Climate and development: enhancing impact through stronger linkages in the implementation of the Paris Agreement and the Sustainable Development Goals (SDGs), Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Sci. 376 (2119) (2018) 20160444, https://doi.org/10.1098/rsta.2016.0444.
[7] Intergovernmental Panel on Climate Change (IPCC), 2023. Climate change 2023 synthesis report: a report of the intergovernmental panel on climate change. URL: https://www.ipcc.ch/report/ar6/syr/downloads/report/IPCC AR6 SYR FullVolume.pdf. https://www.ipcc.ch/report/ar6/syr/downloads/report/IPCC_AR6_SYR_FullVolume.pdf.
[8] World Commission on Environment and Development (WCED), Our Common Future: World Commission on Environment and Development, Oxford University Press, Oxford, 1987.
[9] D. Clifton, Security and a sustainable world, J. Sustain. Dev. 2 (3) (2009), https://doi.org/10.5539/jsd.v2n3p3.
[10] E. Salas Alfaro, M. Wester, P.D. Lama, Exploring the interconnection of sustainability and security in the Global South, a scoping study, Discov. Sustain. 7 (2026) 523, https://doi.org/10.1007/s43621-026-03117-9.
[11] Dutton, A., 2022. 'hedgehog-hunting" thieves who stole solar panels from disabled woman spared jail'. independent. URL: https://www.independent.co.uk/news/uk/crime/solar-panels-robbery-hedgehog-court.
[12] J. Connell, Theft of £100,000 plus solar panels in Bretforton, Evesham J. (2023). URL, https://www.eveshamjournal.co.uk/news/23270349.theft-100-000-plus-solar-panels-b.
[13] Norman, W. UK entering 'peak period' of solar PV theft by 'fully industrialised' criminal network. URL: https://www.solarpowerportal.co.uk/solar-projects/uk-entering-peak-period-of-sol. Accessed on 15 August 2025.
[14] P.H. Gleick, Water and terrorism, Water Policy 8 (2006) 481–503. URL, https://pacinst.org/wp-content/uploads/2013/04/water. and terrorism 2006.pdf.
[15] BBC News, RHI: "Corruption Did Not Cause" Energy Scheme Failure, BBC News, 2020. URL: https://www.bbc.co.uk/news/uk-northern-ireland-51840287.
[16] J.E. Eck, E.B. Eck, Crime place and pollution: expanding crime reduction options through a regulatory approach, Criminol. Public Policy 11 (2012) 281–316.
[17] S.D. Johnson, Identifying and preventing future forms of crimes using situational crime prevention, Secur. J. 37 (2024) 515–534.
[18] L.E. Cohen, M. Felson, Social change and crime rate trends: a routine activity approach (1979). Classics in Environmental Criminology, Routledge, 2010, pp. 203–232.
[19] K. Pease, The Oxford Handbook of Criminology: Crime Reduction, Oxford University Press, 2002.
[20] D.B. Cornish, R.V. Clarke, The Reasoning Criminal: Rational Choice Perspectives On Offending, Transaction Publishers, 2014.
[21] Laycock, G., 2004. The UK car theft index: an example of government leverage. Understanding and preventing car theft 17, 25–44.
[22] J. Gomez-Quintero, S.D. Johnson, H. Borrion, S. Lundrigan, A scoping study of crime facilitated by the metaverse, Futures 157 (2024) 103338, https://doi.org/10.1016/j.futures.2024.103338.
[23] Zheng, S.Y., Johnson, S.D., Pasculli, L., 2026. A scoping review of future crime risks enabled or facilitated by social robots. Under review.
[24] E.A. Akartuna, S.D. Johnson, A. Thornton, Preventing the money laundering and terrorist financing risks of emerging technologies: an international policy Delphi study, Technol. Forecast. Soc. Chang. 179 (2022) 121632, https://doi.org/10.1016/j.techfore.2022.121632.
[25] C.C. Williams, A burning desire: the need for anti-money laundering regulations in carbon emissions trading schemes to combat emerging criminal typologies, J. Money Laund. Control 16 (2013) 298–320.
[26] R.E. McKie, P.B. Stretesky, M.A. Long, Carbon Crime in the Voluntary Market: An Exploration of Modernization Themes Among a Sample of Criminal and Non-Criminal Organizations, 23, Springer, 2015, https://doi.org/10.1007/s10612-015-9294-3.
[27] BBC. Big rise in electric vehicle charging cable thefts. URL: https://www.bbc.co.uk/news/articles/cq5zp064948o. accessed on 15 August 2025.
[28] The Guardian, Windfarms in England hit by wave of copper cabling thefts. URL: https://www.theguardian.com/business/2025/jun/23/windfarms-in-england-hit-by-wav accessed on 15 August 2025.
[29] Initiative, U.E.P.F. Climate Risks in the Metals and Mining Sector. Sectoral Risk Briefings: Insights for Financial Institutions.
[30] N. Bernards, Child labour, cobalt and the London metal exchange: fetish, fixing and the limits of financialization, Econ. Soc. 50 (2021) 542–564.

[31] N. Tuptuk, S. Hailes, Security of smart manufacturing systems, J. Manuf. Syst. 47 (2018) 93–106, https://doi.org/10.1016/j.jmsy.2018.04.007.
[32] The Intergovernmental Panel on Climate Change (IPCC), 2022. Climate change 2022. Mitigation of climate change. URL: https://www.ipcc.ch/report/ar6/syr/downloads/report/IPCC AR6 SYR FullVolume.pdf. https://www.ipcc.ch/report/ar6/wg3/downloads/report/IPCC_AR6_WGIII_FullReport.pdf.
[33] I. Malmio, Can security be sustainable? Three perspectives on security and social sustainability: paradox, co-production, and deconstruction, Sustain. Sci. 19 (2024) 615–627, https://doi.org/10.1007/s11625-023-01450-w.
[34] I. Overland, B.K. Sovacool, The misallocation of climate research funding, Energy Res. Soc. Sci. 62 (2020) 101349, https://doi.org/10.1016/j.erss.2019.101349. URL: https://www.sciencedirect.com/science/article/pii/S2214629619309119.
[35] L. Pasculli, Het recht toekomstbestendig maken, Justitiele Verkenn. 50 (2024).
[36] M.J. Page, J.E. McKenzie, P.M. Bossuyt, I. Boutron, T.C. Hoffmann, C.D. Mulrow, L. Shamseer, J.M. Tetzlaff, E.A. Akl, S.E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hrobjartsson, M.M. Lalu, T. Li, E.W. Loder, E. Mayo-Wilson, S. McDonald, L.A. McGuinness, L.A. Stewart, J. Thomas, A.C. Tricco, V.A. Welch, P. Whiting, D. Moher, The PRISMA 2020 statement: an updated guideline for reporting systematic reviews, BMJ 372 (2021) n71, https://doi.org/10.1136/bmj.n71. URL: https://www.bmj.com/content/372/bmj.n71.
[37] C. Lockwood, Z. Munn, K. Porritt, Qualitative research synthesis: methodological guidance for systematic reviewers utilizing meta aggregation, JBI Evid. Implement. 13 (2015) 179–187.
[38] P. Hillyard, S. Tombs, From 'crime' to social harm? Crime Law Soc. Chang. 48 (2007) 9–25.
[39] R.E. McKie, An Environmental Harm Perspective to Examine our Understanding of UK Nuclear Energy Expansion, 7, Elsevier Sci Ltd, 2020, pp. 556–564, https://doi.org/10.1016/j.exis.2019.10.011.
[40] M. Lynch, P. Stretesky, Smell the death, hear the cries: green victimization and radical-green criminology in the era of global environmental collapse, Radic. Criminol. 6 (2018) 245–277.
[41] P. Stretesky, M. Long, M. Lynch, The Treadmill of Crime: Political Economy and Green Criminology, Routledge, 2013.
[42] L. Tompson, J. Belur, Information retrieval in systematic reviews: a case study of the crime prevention literature, J. Exp. Criminol. 12 (2016) 187–207.
[43] T. Byrt, How good is that agreement? Epidemiology 7 (1996) 561, 561–561URL, http://www.jstor.org/stable/3702168.
[44] T. Byrt, J. Bishop, J.B. Carlin, Bias, prevalence and kappa, J. Clin. Epidemiol. 46 (1993) 423–429, https://doi.org/10.1016/0895-4356(93)90018-V.
[45] V. Braun, V. Clarke, Thematic Analysis, American Psychological Association, 2012.
[46] V. Almagro-Pastor, M. Conradi, T.A. DelValls, I. Riba, Alterations in the Macrobenthic fauna from Guadarranque river (southern Spain) Associated with Sediment-Seawater Acidification Deriving from CO2 leakage, Mar. Pollut. Bull. (2015), https://doi.org/10.1016/j.marpolbul.2015.05.044. PERGAMON-ELSEVIER SCIENCE LTD 96.
[47] Byers, E.A., Hall, J.W., Amezaga, J.M., 2014. Electricity generation and cooling water use: UK pathways to 2050. ELSEVIER SCI LTD 16–30, 25. doi:10.1016/j.gloenvcha.2014.01.005.
[48] H. Eldardiry, E. Habib, Carbon capture and sequestration in power generation: review of impacts and opportunities for water sustainability, BMC 8 (2018), https://doi.org/10.1186/s13705-018-0146-3.
[49] Merschmann, P.R.D.C., Vasquez, E., Szklo, A., re S., Schaeffer, R., 2013. Modeling water use demands for thermoelectric power plants with ccs in selected brazilian water basins. ELSEVIER SCI LTD 87–101, 13. doi:10.1016/j.ijggc.2012.12.019.
[50] L. Rosa, J.A. Reimer, M.S. Went, P. D'Odorico, Hydrological Limits to Carbon Capture and Storage, 3, Ture Portfolio, 2020, https://doi.org/10.1038/s41893-020-0532-7.
[51] Climate Justice Alliance, 2023. Climate justice leaders denounce carbon capture and storage plans as scams, warn reliance on unproven technology exacerbates climate change and environmental injustices. URL: https://climatejusticealliance.org/cj-leaders-denounce-ccs-at-whejac/.
[52] B.K. Sovacool, C. Baum, S. Low, The Next Climate War? Statecraft, Security, and Weaponization in the Geopolitics of a Low-Carbon Future, 45, Elsevier, 2023, https://doi.org/10.1016/j.esr.2022.101031.
[53] D. Rojas-Rueda, K. McAuliffe, E. Morales-Zamora, Addressing Health Equity in the Context of Carbon Capture, Utilization, and Sequestration Technologies, Springer Nature B.V., 2024, pp. 225–237, https://doi.org/10.1007/s40572-024-00447-6. PP - Heidelberg.
[54] Sadawi, A.A., Madani, B., Saboor, S., Ndiaye, M., Abu-Lebdeh, G., 2020. A hierarchical blockchain of things network for unified carbon emission trading (hbuets): a conceptual framework. doi:10.1109/ICTMOD49425.2020.9380610.
[55] Du, C., Wang, Q., Zhang, X., 2024. Optimization method for low carbon economic dispatch of carbon capture power plants considering market power constraint in carbon trading market. doi: 10.1109/CIEEC60922.2024.10583439.
[56] A. Bacci, Carbon capture, Utilization and Storage Tax Credits and Tax Equity Project Financing in the USA: An Assessment Under Bilateral Tax Treaties and BEPS Actions, 16, Oxford University Press, 2023, https://doi.org/10.1093/jwelb/jwad025.
[57] Thirunavukkarasu, H., Rajendran, K., Dinesh, K., Gunasekaran, S., 2023. Application of blockchain and IoT in cap and trade of carbon emissions. doi:10.1109/RAEEUCCI57140.2023.10134302.
[58] Davidson, M.R., Karplus, V.J., Lewis, J.I., Nahm, J., Wang, A., 2022. Risks of decoupling from china on low-carbon technologies. The American Association for the Advancement of Science PP - Washington 1266–1269, 377. doi: 10.1126/science.abq5446.
[59] Jaschke, G., Biermann, F., 2022. The policy discourse on negative emissions, land-based technologies, and the global south. ELSEVIER SCI LTD 102550, 75. doi:10.1016/j.gloenvcha.2022.102550.
[60] Attanasio, L., Conti, M., Donadel, D., Turrin, F., 2021. Miniv2g: an electric vehicle charging emulator. doi: https://doi.org/10.1145/3457339.3457980.
[61] Kumar, B., Mittal, H.K., Rupam, Kaur, G., Rani, Y., Jain, V., 2023. Smart electric cars: navigating the intersection of sustainable innovation and security threats. doi:10.1109/ICACCTech61146.2023.00092.
[62] Jang, C.K., Lee, J., Yi, O., 2017. Encryption scheme in portable electric vehicle charging infrastructure: encryption scheme using symmetric key. doi:10.1109/CAIPT.2017.8320674.
[63] S. Eghtessad, T. Hasanli, R. Huynh, K. Workneh, M.I. Ibrahem, M.M. Fouda, A Survey on Privacy Preservation Methods in Future Vehicular Networks, The Institute of Electrical and Electronics Engineers, Inc. (IEEE), 2023, https://doi.org/10.1109/ICoICT58202.2023.10262771. PP – Piscataway.
[64] Cleveland, F.M., 2008. Cyber security issues for advanced metering infrasttructure (ami). doi:10.1109/PES.2008.4596535.
[65] R. Beheshteh, M. Seyedamirabbas, G. Kambiz, Interconnected and Complex Electric Power and Transportation Systems: A Swot Analysis, 8, Springer Nature B.V., 2021, pp. 207–221, https://doi.org/10.1007/s40518-021-00193-5. PP - Heidelberg.
[66] Rahman, S., Aburub, H., Mekonnen, Y., Sarwat, A.I., 2018. A study of EV BMS cyber security based on neural network soc prediction. doi:10.1109/TDC.2018.8440144.
[67] Wang, W., Memon, F.H., Lian, Z., Yin, Z., Gadekallu, T.R., Pham, Q.V., Dev, K., Su, C., 2023. Secure-enhanced federated learning for ai-empowered electric vehicle energy prediction. 27–34. doi:10.1109/MCE.2021.3116917.
[68] Yuan, H., Li, S., 2022. Cyber security risks of net zero technologies. doi:10.1109/DSC54232.2022.9888883.
[69] Reddy, A.G., Babu, P.R., Odelu, V., Wang, L., Kumar, S.A., 2023. V2g-auth: lightweight authentication and key agreement protocol for v2g environment leveraging physically unclonable functions. doi:10.1109/TICPS.2023.3290539.
[70] Vaidya, B., Mouftah, H.T., 2021. Security for shared electric and automated mobility services in smart cities. 19. doi:10.1109/MSEC.2020.3013759.
[71] Isik, G.K., Tryfonas, T., Oikonomou, G., 2023. E-scooter sharing platforms: understanding their architecture and cybersecurity threats. doi:10.1109/ITSC57777.2023.10421849.
[72] S. Tembo, K.J. Nyoni, Assessing the Ramifications of Electric Vehicle Charging Infrastructure On Smart Grid Systems in Zambia, The Institute of Electrical and Electronics Engineers, Inc. (IEEE), 2022, https://doi.org/10.1109/ICT4DA56482.2022.9971270. PP – Piscataway.
[73] Patel, A.R., Roscia, M., 2023. Assessing the impact of sociopolitical factors on the rollout of freight electric vehicles. doi:10.1109/ICRERA59003.2023.10269373.
[74] Raj, M.J., Gadde, S., Jayaraman, R., 2021. Implementation of biometric access control using fingerprint for safety and security system of electric vehicle. doi:10.1109/ICOSEC51865.2021.9591718.
[75] Badhwar, T., Galodha, A., 2022. Electric vehicles: a comprehensive review on sustainable, financial, political-policy prowess and prospects in India with labor policies of china and Africa. doi: 10.1109/IPRECON55716.2022.10059516.
[76] B.K. Sovacool, Who Are the Victims of Low-Carbon Transitions? Towards a Political Ecology of Climate Change Mitigation, 73, Elsevier, 2021, https://doi.org/10.1016/j.erss.2021.101916.
[77] Tabuchi, H., Plumer, B., 2021. How green are electric vehicles?
[78] Huber, S.T.W., Steininger, K.W., 2022. Critical sustainability issues in the production of wind and solar electricity generation as well as storage facilities and possible solutions. ELSEVIER SCI LTD 130720, 339. doi:10.1016/j.jclepro.2022.130720.
[79] Elsayed, A.A.E., Farag, H.E.Z., Asif, A., 2023. Cyber physical security of energy hubs using feasibility area estimation. doi:10.1109/ITCEgypt58155.2023.10206242.
[80] Z. Allal, H.N. Noura, O. Salman, K. Chahine, Machine Learning Solutions For Renewable Energy Systems: Applications, Challenges, Limitations, and Future Directions, Academic Press Ltd- Elsevier Science Ltd, 2024 120392, https://doi.org/10.1016/j.jenvman.2024.120392.
[81] M. Asif, G. Naeem, M. Khalid, Digitalization For Sustainable Buildings: Technologies, Applications, Potential, and Challenges, 450, Elsevier Sci Ltd, 2024, https://doi.org/10.1016/j.jclepro.2024.141814.
[82] U. Cali, F.O. Catak, U. Halden, Trustworthy Cyber-Physical Power Systems Using AI: Dueling Algorithms for PMS Anomaly Detection and Cybersecurity, 57, Springer, 2024, https://doi.org/10.1007/s10462-024-10827-x.
[83] M. Faheem, M.A. Al-Khasawneh, Multilayer Cyberattacks Identification and Classification Using Machine Learning in Internet of Blockchain (IOBC)-Based Energy Networks, 54, Elsevier, 2024, https://doi.org/10.1016/j.dib.2024.110461.
[84] V.A. Greiman, Nuclear Cyber Attacks: A Study of Sabotage and Regulation of Critical Infrastructure, Academic Conferences International Limited, 2023. PP – Reading.
[85] Ahmed, M., Farooq, M.S., ul Haque, M.I., Ahmed, M., Maqbool, H., Yousaf, A., 2021. Application of blockchain in green energy for sustainable future. doi:10.1109/ICEET53442.2021.9659727.
[86] Mishra, N., Kumar, V., Bhardwaj, G., 2019. Role of cloud computing in smart grid. doi:10.1109/ICACTM.2019.8776750.
[87] Zivic, N.S., Ur-Rehman, O., Ruland, C., 2015. Evolution of smart metering systems. doi:10.1109/TELFOR.2015.7377547.
[88] A. Rekeraho, D.T. Cotfas, P.A. Cotfas, E. Tuyishime, T.C. Balan, R. Acheampong, Enhancing Security for IoT-Based Smart Renewable Energy Remote Monitoring

Systems, MDPI AG, 2024, p. 756, https://doi.org/10.3390/electronics13040756. PP - Basel.
[89] Aziz, S., Joseph, M.K., Ferreira, H.C., 2017. A model for cloud-based large scale smart grid technologies. doi:10.1109/EEEIC.2017.7977398.
[90] Chakraborty, S., Mombeshora, E.M., Clark, K.P., Mbavarira, T.S., 2024. Understanding of cyber-attack vulnerabilities during natural disasters and discussing a cyber-attack resiliency framework. doi: 10.1109/SoutheastCon52093.2024.10500233.
[91] Pareek, S., Kuhar, S., Meena, G.K., Pathani, A., Akhayyat, A., Kumar, R., 2023. Smart cities: exploring the advancement and challenges in urbanization. doi:10.1109/CISCT57197.2023.10351466.
[92] Yazdanipour, S., Arani, F.M., Jahromi, A.A., 2024. Investigating cyberattacks against off-grid solar-powered electric vehicle charging stations. doi: 10.1109/TD47997.2024.10556091.
[93] Ahmed, W., 2017. Evaluating high performance computing (hpc) requirements of devices on the smart grid for increased cybersecurity. doi:10.1109/Anti-Cybercrime.2017.7905272.
[94] Chen, Y.T., Ko, Y.C., 2014. Determine information security features for smart grid through constructing a threat model. doi:10.1109/SII.2014.7028133.
[95] Pourmirza, Z., Walker, S., 2021. Electric vehicle charging station: cyber security challenges and perspective. doi:10.1109/SEGE52446.2021.9535052.
[96] Q. Zhang, F. Li, J. Zhao, B. She, False Data Injection Attack and Corresponding Countermeasure in Multienergy Systems, 39, The Institute of Electrical and Electronics Engineers, Inc. (IEEE), 2024, https://doi.org/10.1109/TPWRS.2023.3276736. PP - New York.
[97] Sayali, S.S., Thakre, M.P., Chandrakant, S., Jain, A.M., Ganesh, M., 2020. Functionality of smart grid with re enables the generation of solar energy: opportunity to come. doi: 10.1109/ICPECTS49113.2020.9337019.
[98] Kivimaa, P., Brisbois, M.C., Jayaram, D., Hakala, E., Siddi, M., 2022. A socio-technical lens on security in sustainability transitions: future expectations for positive and negative security. ELSEVIER SCI LTD 102971, 141. doi:10.1016/j.futures.2022.102971.
[99] Zhang, D., Li, C., Goh, H.H., Ahmad, T., Zhu, H., Liu, H., Wu, T., 2022. A comprehensive overview of modeling approaches and optimal control strategies for cyber-physical resilience in power systems. PERGAMONELSEVIER SCIENCE LTD 1383–1406, 189. doi:10.1016/j.renene.2022.03.096.
[100] O.I. Falowo, J. Kropczynski, C. Li, Protecting Critical Infrastructure: Strategies for Managing Cybersecurity Risks in Nuclear Fusion Facilities, The Institute of Electrical and Electronics Engineers, Inc. (IEEE), 2023, https://doi.org/10.1109/ISPA-BDCloud-SocialComSustainCom59178.2023.00170. PP - Piscataway.
[101] A. Gambhir, R. Lempert, From least cost to least risk: producing climate change mitigation plans that are resilient to multiple risks, Front. Media SA 5 (2023), https://doi.org/10.3389/fclim.2023.1149309.
[102] S. Dorji, A.A. Stonier, P. Geno, R. Kuppusamy, Y. Teekaraman, An Extensive Critique On Smart Grid Technologies: Recent Advancements, Key Challenges, and Future Directions, MDPI AG, 2023, p. 11, https://doi.org/10.3390/technologies11030081. PP – Basel.
[103] E.B. Ali, V.P. Anufriev, B. Amfo, Green Economy Implementation in Ghana as a Road Map for a Sustainable Development Drive: A Review, 12, Elsevier, 2021, https://doi.org/10.1016/j.sciaf.2021.e00756.
[104] Chen, F.F., Wang, Q.S., Umar, M., Zheng, L., 2023. Towards sustainable resource management: the role of governance, natural resource rent and energy productivity. ELSEVIER SCI LTD 104026, 85. doi:10.1016/j.resourpol.2023.104026.
[105] D. Chirambo, Towards the Achievement of SDG 7 in Subsaharan Africa: Creating Synergies Between Power Africa, Sustainable Energy for All and Climate Finance In-Order to Achieve Universal Energy Access Before 2030, Pergamon-Elsevier Science Ltd, 2018, pp. 600–608, https://doi.org/10.1016/j.rser.2018.06.025.
[106] M. Engelken, B. Roemer, M. Drescher, I.M. Welpe, A. Picot, Comparing Drivers, Barriers, and Opportunities of Business Models for Renewable Energies: A Review, 60, Pergamon-Elsevier Science Ltd, 2016, https://doi.org/10.1016/j.rser.2015.12.163.
[107] Khan, Y., Hassan, T., 2024. Promoting sustainable development: evaluating the influence of natural resources, high-tech export and corruption on co¡sub¿2¡/sub¿ emissions in developing economies. ELSEVIER SCI LTD 104511, 88. doi:10.1016/j.resourpol.2023.104511.
[108] Kwakwa, P.A., 2023. Climate change mitigation role of renewable energy consumption: does institutional quality matter in the case of reducing Africa's carbon dioxide emissions? ACADEMIC PRESS LTD- ELSEVIER SCIENCE LTD 118234, 342. doi:10.1016/j.jenvman.2023.118234.
[109] Kivyiro, P., Arminen, H., 2013. Exploring the factors affecting the clean development mechanism in the developing countries. doi:10.1109/EEM.2013.6607316.
[110] S. Ren, Y. Hao, H. Wu, Government Corruption, Market Segmentation and Renewable Energy Technology Innovation: Evidence from China, Academic Press Ltd- Elsevier Science Ltd, 2021 113686, https://doi.org/10.1016/j.jenvman.2021.113686.
[111] Shahnazi, R., Alimohammadlou, M., 2022. Investigating risks in renewable energy in oil-producing countries through multi-criteria decision-making methods based on interval type-2 fuzzy sets: a case study of iran. PERGAMON-ELSEVIER SCIENCE LTD 1009–1027. doi:10.1016/j.renene.2022.04.051.
[112] Liu, F., Xia, Z., Lee, C.C., 2024. Does green credit benefit the clean energy technological innovation and how? The policy catering behavior of enterprises. ELSEVIER SCI LTD 141256, 444. doi:10.1016/j.jclepro.2024.141256.
[113] A.O. Acheampong, E.E.O. Opoku, K.E. Dogah, The Political Economy of Energy Transition: The Role of Globalization and Governance in the Adoption of Clean Cooking Fuels and Technologies, 186, Elsevier Science Inc, 2023, https://doi.org/10.1016/j.techfore.2022.122156.
[114] R. Hamann, B. Rennkamp, W. Kruger, J.K. Musango, Corruption Undermines Justice in Clean Energy Transitions, Kirkpatrick Jordon Foundation, PP - Washington, 2023, p. 65.
[115] Jepng'etich, K.S., 2020. Sustainable fuelwood production in Kenya: potential role of community forest associations. doi:10.1109/ICUE49301.2020.9307096.
[116] A.R. Pfadt-Trilling, M.O.P. Fortier, Greenwashed Energy Transitions: Are us Cities Accounting for the Life Cycle Greenhouse Gas Emissions of Energy Resources in Climate Action Plans? Elsevier, 2021, p. 2, https://doi.org/10.1016/j.egycc.2020.100020.
[117] V. Pop, EU Sustainable Finance Rules to Defy Greenwashing Accusations, The Financial Times Limited, PP - London, 2022.
[118] A. Vlachou, G. Pantelias, The EU'S Emissions Trading System, Part 2: A political Economy Critique, Taylor & Francis Ltd, PP - Abingdon, 2017, pp. 108–127, https://doi.org/10.1080/10455752.2016.1234027.
[119] Hughes, S.S., Velednitsky, S., Green, A.A., 2023. Greenwashing in palestine/israel: settler colonialism and environmental injustice in the age of climate catastrophe. SAGE PUBLICATIONS INC 495–513, 6. doi:10.1177/25148486211069898.
[120] D. Andreucci, C. Zografos, Between Improvement and Sacrifice: Othering and the (Bio)political Ecology of Climate Change, Elsevier Sci Ltd, 2022 102512, https://doi.org/10.1016/j.polgeo.2021.102512.
[121] M. Kiehbadroudinezhad, H. Hosseinzadeh-Bandbafha, M.A. Rosen, V.K. Gupta, W. Peng, M. Tabatabaei, M. Aghbashlo, The Role of Energy Security and Resilience in the Sustainability of Green microgrids: Paving the Way to Sustainable and Clean Production, 60, Elsevier, 2023, https://doi.org/10.1016/j.seta.2023.103485.
[122] F. Boamah, Desirable Or Debatable? Putting Africa's Decentralised Solar Energy Futures in Context, 62, Elsevier, 2020, https://doi.org/10.1016/j.erss.2019.101390.
[123] South African Institute of Chartered Accountants, Renewable Energy Companies Linked to Human Rights Abuse, South African Institute of Chartered Accountants, 2019. PP - Johannesburg.
[124] M. Copley, Solar-Panel Supplier's Links to Alleged Abuses in China Imperil us Climate Goal, SNL Financial LC, 2021. PP – Charlottesville.
[125] B.E.K. Nsafon, N.N. Same, A.O. Yakub, D. Chaulagain, N.M. Kumar, J.S. Huh, The justice and policy implications of clean energy transition in Africa, Front. Media SA 11 (2023), https://doi.org/10.3389/fenvs.2023.1089391.
[126] A. Dunlap, M. Riquito, Social Warfare for Lithium Extraction? Open-Pit Lithium Mining, Counterinsurgency Tactics and Enforcing Green Extractivism in Northern Portugal, 95, Elsevier, 2023, https://doi.org/10.1016/j.erss.2022.102912.
[127] J. Charles Rajesh Kumar, D. Vinod Kumar, D. Baskar, B. Mary Arunsi, R. Jenova, M.A. Majid, Offshore Wind Energy Status, Challenges, Opportunities, Environmental Impacts, Occupational Health, and Safety Management in India, Sage Publications Ltd, 2021, pp. 565–603, https://doi.org/10.1177/0958305X20946483.
[128] S. Ferrey, Sustainable Development Arrested by U.S. Criminal Law, American University Law Review, 2019, p. 68. PP - Washington.
[129] J. Lloret, A. Turiel, J. Sole, E. Berdalet, A. Sabates, A. Olivares, J.M. Gili, J. Vila-Subiros, R. Sarda, Unravelling the Ecological Impacts of Large-Scale Offshore Wind Farms in the Mediterranean Sea, 824, Elsevier, 2022, https://doi.org/10.1016/j.scitotenv.2022.153803.
[130] C. Soria-Rodriguez, Marine Renewable Energy Technologies on the High seas: Challenges and Opportunities to Strengthen International Environmental and Renewable Energy Governance, Edward Elgar Publishing Ltd, 2022, p. 11, https://doi.org/10.4337/cilj.2022.02.03.
[131] R. Dautray, J. Friedel, Y. Brechet, Nuclear Energy in France Today and Tomorrow: IInd to IVth Generations, Elsevier, 2012, p. 13, https://doi.org/10.1016/j.crhy.2012.02.001. FRANCE-EDITIONS SCIENTIFIQUES MEDICALES ELSEVIER.
[132] S.K. Jain, Inevitability of Nuclear Power in the Asian Region - Asian nuclear Prospects 2010, 7, Elsevier Science BV, 2011, https://doi.org/10.1016/j.egypro.2011.06.003.
[133] S.D. Schmid, A New "Nuclear Normalcy"? Sage Publications Ltd, 2019, pp. 297–315, https://doi.org/10.1177/1755088218796674.
[134] B. Sertyesilisik, Y. Melaine, Nuclear Power in the Global Warming Era: Environmental, Economic, and Policy Considerations, Wiley Periodicals Inc, PP - Hoboken, 2010, p. 19.
[135] Duffey, R.B., Torgerson, D.F., Miller, A.I., Hopwood, J., 2006. Canadian solutions to global energy and environment challenges: green atoms. doi:10.1109/EICCCC.2006.277186.
[136] Limpens, G., Nalubega, J., Waibale, F., 2022. Providing renewable energy to rural areas: intervention in nine colleges in Uganda. doi:10.1109/PowerAfrica53997.2022.9905380.
[137] Zheng, J., 2023. Research on anti-stealing algorithm of distributed photovoltaic power system based on power big data. doi:10.1109/ICIRDC62824.2023.00147.
[138] Sivasankaran, S., Jebaraj, B.S., 2022. Battery power optimization and theft detection system in electric tractor. doi:10.1109/IC3IOT53935.2022.9767910.
[139] Merlin, S.S., Yugha, R., Hubert Mary, L., Varalakshmi, P., Mavaluru, D., 2023. A hybrid deep learning neural network model and data-driven methods for smart grid theft detection. doi:10.1109/ICSES60034.2023.10465331.
[140] M.W. Jones, G.P. Peters, T. Gasser, R.M. Andrew, C. Schwingshackl, J. Gütschow, R.A. Houghton, P. Friedlingstein, J. Pongratz, C. Le Quéré, National contributions to climate change due to historical emissions of carbon dioxide, methane, and nitrous oxide since 1850, Sci. Data 10 (2023) 155.

[141] D. Welsby, J. Price, S. Pye, P. Ekins, Unextractable fossil fuels in a 1.5 c world, Nature 597 (2021) 230–234.
[142] R.V. Clarke, Situational crime prevention, Crime Justice 19 (1995) 91–150.
[143] K. Mortezaei, A. Amirlatifi, E. Ghazanfari, F. Vahedifard, Potential CO2 leakage from geological storage sites: advances and challenges, Environ. Geotech. 8 (2021) 3–27, https://doi.org/10.1680/jenge.18.00041.
[144] J.M. Bielicki, M.F. Pollak, J.P. Fitts, C.A. Peters, E.J. Wilson, Causes and financial consequences of geologic CO2 storage reservoir leakage and interference with other subsurface resources, Int. J. Greenh. Gas Control 20 (2014) 272–284, https://doi.org/10.1016/j.ijggc.2013.10.024. URL: https://www.sciencedirect.com/science/article/pii/S1750583613003770.
[145] Z. Rui, L. Zeng, B. Dindoruk, Challenges in the largescale deployment of CCUS, Engineering 44 (2025) 17–20, https://doi.org/10.1016/j.eng.2024.11.031. URL: https://www.sciencedirect.com/science/article/pii/S2095809924007203.
[146] Li, P., Yang, J., Islam, M.A., Ren, S., 2023. Making AI less" thirsty": uncovering and addressing the secret water footprint of AI models. arXiv preprint arXiv: 2304.03271.
[147] M. Bindl, M.R. Edwards, R.Y. Cui, Risks of relying on uncertain carbon dioxide removal in climate policy, Nat. Commun. 16 (2025), https://doi.org/10.1038/s41467-025-61106-4.
[148] P. Higgins, D. Short, N. South, Protecting the planet: a proposal for a law of ecocide, Crime Law Soc. Chang. 59 (2013) 251–266.
[149] Webster, J., Leung, Z., Beijing's plan for Taiwan challenges its offshore wind push. URL: https://www.lowyinstitute.org/the-interpreter/beijing-s-plan-taiwan-challenges-i. Accessed on 2 July 2025.
[150] P. Ekblom, Designing products against crime, in:. Handbook of Crime Prevention and Community Safety, Willan, 2013, pp. 229–270.